ВИСШЕ УЧИЛИЩЕ ПО СИГУРНОСТ
И ИКОНОМИКА – ПЛОВДИВ
HIGHER SCHOOL OF SECURITY AND ECONOMICS – PLOVDIV, BULGARIA

НАУЧНОТЕОРЕТИЧНА КОНФЕРЕНЦИЯ

БЪЛГАРСКОТО РАЗУЗНАВАНЕ И КОНТРАРАЗУЗНАВАНЕ

предизвикателства, проблеми, перспективи

11 април 2025 г.

SCIENTIFIC AND THEORETICAL CONFERENCE

BULGARIAN INTELLIGENCE AND COUNTERINTELLIGENCE

challenges, problems, perspectives

April 11, 2025

ИЗДАТЕЛСКИ КОМПЛЕКС ВУСИ

ВИСШЕ УЧИЛИЩЕ ПО СИГУРНОСТ И ИКОНОМИКА

СБОРНИК С ДОКЛАДИ

ОТ НАУЧНОТЕОРЕТИЧНАТА КОНФЕРЕНЦИЯ

НА ТЕМА

БЪЛГАРСКОТО РАЗУЗНАВАНЕ И КОНТРАРАЗУЗНАВАНЕ

ПРЕДИЗВИКАТЕЛСТВА, ПРОБЛЕМИ, ПЕРСПЕКТИВИ

11 април 2025 г.

Пловдив, 2025

Предложените материали отразяват личната позиция на авторите и не ангажират с нея Редакционната колегия на сборника.

ISBN (Print) 978-619-7774-24-5
ISBN (ePub) 978-619-7774-25-2
ISBN (pdf) 978-619-7774-26-9

СЪДЪРЖАНИЕ

СЪВРЕМЕННОТО РАЗУЗНАВАНЕ И КОНТРАРАЗУЗНАВАНЕ И СЛУЖБИТЕ ЗА СИГУРНОСТ И ОБЩЕСТВЕН РЕД – ИСТОРИЯ, СЪСТОЯНИЕ, ВИЗИЯ ЗА РАЗВИТИЕ

ПРИВЕТСТВИЕ

Уважаеми гости и участници в конференцията,

Позволете ми да Ви приветствам с „Добре дошли!“ във Висшето училище по сигурност и икономика, изразявайки своето огромно задоволство от това, че уважихте нашия научен форум. Тематиката на конференцията, която третира проблемите на българското разузнаване, вълнува всички, поради което неслучайно сме се спрели на нея. Според нас тази проблематика днес става все по-актуална, поради което тя непрекъснато трябва да се интерпретира, анализира и осмисля в контекста на съвременните геополитически реалности и мощни турбулентни процеси, които се развиват в тази сфера. Защото независимо от десетилетните демократични промени в страната за разузнаването и службите за сигурност се говори плахо, прекалено малко и направо пренебрежително, сякаш те не са ключови структури на съвременната държава, а някакви невзрачни административни органи, работещи на тъмно. Нещо повече – специално в България все още битува порочната теза, че след като членуваме в два могъщи съюза (ЕС и НАТО), ролята и мястото на разузнаването вече не са толкова важни, тъй като нашите предишни врагове вече са ни партньори и приятели. Това е била една от целите, когато решихме да се спрем на едно такова заглавие. И още по-конкретно – да се опитаме да изясним задълбочено с помощта на обективния научен анализ какво е състоянието на българското разузнаване днес, какви са неговите основни проблеми и пред какви предизвикателства е изправено то. В този контекст сме дълбоко убедени, че ни предстои сериозна научна дискусия, която да засегне цялата гама проблеми в българския разузнавателен сектор и която въз основа на „кривиците“ в нашите служби за сигурност да направи адекватни изводи и препоръки за тяхното качествено развитие у нас, на Балканите, в Европа и по света.

Убеден съм, че ще влезем в дълбоките полоси на сериозната научна дискусия, от която всички ще имаме полза, с различните тези и идеи в тази област. В крайна сметка да направим така, че действително да има полза от нашия научен форум. Имаме сериозно присъствие на ръководни представители от университетите от 5 държави, с които си партнираме от години, както и от почти всички големи български университети, които обучават студенти в сферата на сигурността (МВР, Военната академия, БАН, УНСС, ПУ „Паисий Хилендарски“ и др.). Така задълбочаваме нашето сътрудничество в рамките на обединена Европа и на балканските държави с нашите колеги, за да поемем всички онези отговорности като ръководители и като учени, които имаме във връзка с решаването на тази проблематика, колкото трудна, щекотлива и деликатна да е тя. Защото разузнаването не е грижа само на държавата – то е дело както на обществото, така и на всички български граждани.

Желая успех на конференцията!

проф. д.п.н. Георги Манолов
президент на ВУСИ

НАЦИОНАЛНАТА СИСТЕМА ЗА РАЗУЗНАВАНЕ – ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ

доц. д-р Васил Станков, проф. д-р Йордан Бакалов
Висше училище по сигурност и икономика – Пловдив

THE NATIONAL INTELLIGENCE SYSTEM – CHALLENGES AND PERSPECTIVES

Assoc. Prof. Vasil Stankov, PhD, Prof. Yordan Bakalov, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Статията изследва предизвикателствата пред националната система за разузнаване и изискванията към нея, като се имат предвид тенденциите в националния разузнавателен процес. В контекста на националната разузнавателна политика се предлага приемането на доктрина на националното разузнаване и провеждането на периодични прегледи на националната система за разузнаване. Анализират се връзките държавно ръководство – разузнавателни служби и разузнаване – гражданско общество. В заключение е посочена необходимостта от иновативни подходи, ясно очертана разузнавателна политика и постоянно адаптиране към оперативната среда.*

Ключови думи: *разузнавателен процес; система за разузнаване; доктрина; прегледи; гражданско общество*

Abstract: *The article explores the challenges and concerns the national intelligence system faces nowadays, given the trends in the national intelligence process. Discussing the national intelligence policy, the article advises the adoption of a National Intelligence Doctrine, as well as periodic reviews of the National Intelligence System. The article goes on to contemplate the liaison between the Intelligence System, state leadership and civil society. The article concludes by highlighting the need for innovative approaches, a clearly outlined intelligence policy and a continuing adaptation to the operational environment.*

Key words: *intelligence process; intelligence system; doctrine; reviews; civil society*

Въведение

Разузнаването и контраразузнаването са средства за постигане на сигурност чрез знание. Това знание е в основата на информирани действия, предназначени да защитят сигурността на гражданите и държавата. Националният разузнавателен процес е проявление на обединението около националните интереси и израз на общия стремеж за гарантиране на развитието и благосъстоянието на обществото. Националната система за разузнаване, която обединява службите за сигурност и службите за обществен ред, е жизненоважна част от системата за защита на националната и съюзната сигурност.

Политиката на разузнаването е най-зле разбирана, а професията на разузнавача си остава неразбрана от политиците. Президентът Кенеди най-добре отбелязва този факт, като заявява: „Вашите успехи остават неизвестни, а вашите провали се разтръбяват“. Похватите и всичко, което се определя като „изкуство на разузнаването“, са известни и общовалидни независимо от националността на службата.

Необходимостта от адекватен отговор на динамичните, сложни и противоречиви процеси във външната и вътрешната среда на сигурност обективно води до на-

растване на значимостта на националната система за разузнаване за ефективното управление и функциониране на националната сигурност. Високата конфликтност в международните отношения, нарасналата тежест на външните военнополитически фактори, задълбочаването на асиметричните и хибридните заплахи налагат активно осъществяване на разузнавателната дейност в нейните три функционални области – външно разузнаване; контраразузнаване; опазване на вътрешната сигурност и обществения ред. Не можем да очакваме, че ще можем да защитим сигурността си, ако противниците ни са убедени, че могат да ни изненадат където и когато пожелаят.

През следващите години ще бъдем свидетели на все по-голямо съсредоточаване на усилията върху дейностите, свързани с информационното осигуряване на външната и отбранителната политика, пресичането на дейността на чуждите разузнавания, гарантирането на многобройните аспекти на вътрешната сигурност и опазването на обществения ред. Все повече ще се засилва ролята на разузнаването като средство за избор на стратегия в отговор на настъпилите или очакваните промени във външната и вътрешната среда на сигурност.

Според обхвата на целите на разузнаването то може да се разглежда като оперативно-тактическо и стратегическо. Важно значение за разузнавателната дейност са международните отношения и националните интереси в конкретни области. Интересите на чужди разузнавателни служби са обусловени от преки глобални, регионални, политически, икономически и етнически фактори. От системата за разузнаване ще се изисква да предвижда промените в средата на сигурност и при настъпването им да бъде готова с решенията за тях. Колкото е по-силно противопоставянето между разузнаващата и разузнаваната страна, толкова е по-мащабна и интензивна разузнавателната дейност.

В зависимост от различните форми на държавно устройство специалните служби имат своите специфични характеристики по отношение на компетентност, задачи, функции, както и място в системата за национална сигурност. Те се създават в рамките на държавните организации и имат за цел да задоволяват обществените потребности при реализирането на определени политики от изпълнителната власт. Разузнавателните служби са органи на изпълнителната власт и благодарение на това имат неразривна връзка с външната и вътрешната политика на държавата, като целта им е да се постигне стратегическо превъзходство над разузнаваните държави. Става въпрос за много сложен комплекс от прилагани дейности, започвайки от дипломацията и свършвайки с войната. Според Карл фон Клаузевиц войната е продължение на политиката с други средства. Точно заради това се прилага комбиниране на различни средства – за да се защити националният ни интерес, и тогава може да е необходимо провеждането на тайни операции между дипломацията и войната. Специалните служби са инструмент на външната и отбранителната политика заедно с дипломацията и въоръжените сили.

Тенденции и изисквания към системата за разузнаване

Най-важната характеристика на системата ще бъде постоянният процес на адаптация към промените в средата на сигурност и към оперативната обстановка. Този процес ще се изразява в усъвършенстване на дейностите, методите, способите и формите на работа с цел обновяване на системата и повишаване на нейната ефективност.

Националният разузнавателен процес ще се организира и осъществява под влиянието на следните по-важни ***тенденции:***

1. Засилване на предупредителната и прогнозиращата функция на разузнаването и контраразузнаването

Необходимостта от ранно предупреждение и превенция обективно ще нараства, което изисква добиване, обработване и анализ на голямо количество разнообразни по характер и съдържание сведения относно потенциални и реални заплахи, предизвикани от взаимносвързани фактори. Това налага увеличаване на способностите за добиване на изпреварваща информация, както и наличие на силен информационно-аналитичен апарат. Бързото протичане на процесите в условията на различни по характер кризисни ситуации ще изисква съкращаване на продължителността на разузнавателния цикъл: добиване – обработване – предоставяне (разпространение) – управление (ръководство и планиране).

Необходимо е много по-бързо да се обработват данните, да се намали времето за ориентация, решение и действие. Колкото този цикъл е по-кратък, толкова по-своевременни и ефективни ще бъдат действията на изпълнителната власт. За да се постигне това, е необходимо разузнаващата страна да е информационно осигурена. Разузнаващата страна чрез своите служби може активно да влияе на вътрешнополитическата обстановка, на външнополитическите позиции и авторитета на разузнаваната държава.

2. Задълбочаване на взаимодействието между службите в рамките на разузнавателната общност

Това е продиктувано от многообразието и широкия обхват на рисковете и заплахите, което от своя страна води до сближаване на функционалните области на разузнаването. Взаимодействието изисква оптимално разпределение на задачите, обща и непосредствена координация на съвместните дейности, прецизно очертаване на правомощията чрез разработване на подробна нормативна уредба за самите разузнавателни служби, както и тяхното взаимодействие. Колкото е по-изчерпателна нормативната уредба в тази си част, толкова е по-трудно службите да излязат от тези рамки. Отношението ни като държава и общество към разузнавателните ни служби и тяхното взаимодействие е показателно за нашите приоритети и за разпределението на силите и средствата, които притежаваме, за да реализираме стратегическите си цели и задачи.

3. Нарастване на значимостта на разузнавателната информация в интерес на отбраната

Значението на разузнавателната информация във военната област значително нараства при външнополитически кризи и при опасност от възникване на военен конфликт. Въоръжената конфронтация в близки до нас региони и цялостното увеличаване на конфликтния потенциал обективно водят до по-голямо влияние на военните аспекти на сигурността.

Превантивната функция на военното разузнаване ще изисква постоянно добиване на сведения не само за системата за отбрана и въоръжените сили на възможните противостоящи страни, а и за останалите компоненти на националната мощ. По този начин оценките и решенията на стратегическо и оперативно-тактическо ниво ще бъдат в по-пълна степен осигурени в информационно отношение.

Разузнаването има ключова роля в съвременните и бъдещите операции и затова са необходими сили и средства с определени характеристики и способности, за да бъдат покрити всички елементи на бойното пространство. За целта ще се използват както национални, така и съюзни средства и способности. Формирането на своевременна, пълна и опозната картина на бойното пространство е основна предпоставка за планирането и воденето на операциите на въоръжените сили.

Основната цел на разузнаването е преди всичко добиване на информация за военния потенциал на разузнаваната страна. Службите за разузнаване се стремят да въздействат на военната политика и чрез дезинформиране на разузнаваната държава, за да вземе неправилни решения, което в крайна сметка да доведе до вътрешни противоречия и да предизвика разногласия в колективната сигурност, в която тя участва.

Не на последно място службите могат да бъдат използвани за проваляне на поръчки за военно оборудване, както и за придобиване на такова оборудване.

4. Засилване на сътрудничеството с разузнавателните органи на НАТО и ЕС и със службите на съюзническите и партньорските държави

Това е абсолютен императив, който налага активизиране на разузнавателното взаимодействие с нашите съюзници във всички направления – обмен на разузнавателна информация, провеждане на съвместни операции, обмен на опит в различни области.

Тези тенденции ще предявят следните ***изисквания*** към системата на националното разузнаване и конкретно към работата на службите за сигурност и обществен ред:

1. По-силна обвързаност на системата за разузнаване с общата политика за сигурност на държавата

Тук възниква въпросът за националната политика в областта на разузнаването: как се формира, планира, съгласува, координира и реализира тази политика и дали трябва да има национален основополагащ документ, например концепция, доктрина или стратегия за националното разузнаване. Възможната цел на този документ е да интегрира подходите и да очертае приоритетите в рамките на националния разузнавателен процес; да обедини възгледите и да консолидира усилията на националната разузнавателна общност. Неговата роля и значимост най-общо се изразяват в следното:

- дефиниране на мисията, визията и общите цели на националната разузнавателна общност;

- определяне на принципите, функциите и механизмите на обществения, гражданския и институционалния контрол върху системата на националното разузнаване;

- създаване на условия за консолидиране на националния разузнавателен процес чрез концептуално обединяване на неговите четири функционални направления (външно разузнаване, контраразузнаване, разузнаване в интерес на вътрешната сигурност и обществения ред, операции за активно въздействие);

- определяне на насоки за развитие на националните разузнавателни способности като един от главните инструменти на политиката за сигурност в съвременната сложна среда.

Заслужава внимание тезата, че за държава като нашата е важно да има единна система за национално разузнаване, чиито елементи се намират в тясно взаимодействие помежду си.

Доктрината ще създаде условия за това чрез сближаване на теоретичните възгледи, стандартизиране на практикоприложните подходи, съвместяване на оперативно-разузнавателните процедури и унифициране на разузнавателната терминология в рамките на разузнавателната общност.

2. Прегледи на националната система за разузнаване

Създаването на култура на периодични прегледи на националната система за разузнаване ще допринесе за адаптиране на системата към промените в средата на сигурност и за усъвършенстване на националния разузнавателен процес.

Прегледът може да включва анализ и оценка на правнонормативната уредба, на програмите и плановете за развитие на способностите на службите за сигурност и обществен ред в дългосрочен период. В основата на прегледа е оценката на рисковете и заплахите, които оказват влияние върху националните потребности от разузнавателна информация. Прегледът може да бъде мотивиран от следните цели или намерения:

- да се подобри държавната политика в областта на разузнаването;

- да се направи оценка на националния разузнавателен процес чрез преглед на дейностите и структурите;

- да се създадат нови разузнавателни способности или да се оптимизират съществуващите чрез преориентиране на силите, средствата и ресурсите;

- да се направи оценка на доктриналните документи и на действащото законодателство.

Прегледът може да се проведе като част от периодичните стратегически прегледи на системата за защита на националната сигурност или като самостоятелен процес под общото ръководство на Съвета по сигурността към МС. Следва да завърши с приемането на планиращи документи, които ще определят насоките на разузнавателната политика, приоритетите на националния разузнавателен процес и изграждането на способности за относително дълъг период от време [3: 18 – 23]. Структурните промени невинаги са необходими и желателни, но при нужда усилията трябва да се пренасочват в приоритетните направления. Трябва да има баланс между наложителните промени и необходимостта от стабилност на дейностите и структурите.

Това е механизъм за трайно решаване на редица проблеми на системата за разузнаване:

✓ Подобряване на правилата, практиките и процедурите за използване на лица източници. Това се налага от нарастващото значение на информацията, добита чрез оперативно-разузнавателна дейност. Разбира се, трябва да се отчита спецификата във функционалните области (външното разузнаване, контраразузнаването, вътрешната сигурност и обществения ред).

✓ Усъвършенстване на системата за привличане на кадри за видовете разузнаване и тяхната подготовка. Развитието и усъвършенстването на системата за разузнаване са невъзможни без достатъчно на брой високоподготвени и мотивирани кадри, които да осигурят качествено изпълнение на задачите в сложна обстановка.

✓ Технологичното обновяване на всички видове разузнаване. Настоящите условия за водене на разузнаване изискват все по-активно използване на оперативно-техническите средства (средства на оперативната техника), както и средствата за техническо събиране и обработване на разузнавателна информация, на първо място електронното разузнаване и разузнаването чрез изображения (ЕР и РИ). „Ерата на интелекта“ разкрива много нови възможности [1: 16], но предявява и нови изисквания.

3. Засилване на връзката държавно ръководство – разузнавателни служби

Държавното ръководство трябва да осъзнава необходимостта от изграждането на ефективна система за разузнаване, като се използват капацитетът и възможностите както на институциите, така и на всеки, който може да допринесе за просперитета на държавата. Това е най-важната предпоставка за качеството на управлението, контрола и отчетността на системата за разузнаване. За да може ефективно да използва разузнаването като инструмент на управлението, от държавното ръководство следва да се очаква:

а) да се отнася към разузнаването като към инструмент за реализиране на националните интереси и секторните политики за сигурност;

б) да притежава висока разузнавателна култура, което означава да има задълбочено разбиране за същността, функциите, дейностите и способностите на националното разузнаване;

в) активно да упражнява правомощията си във връзка с управлението, осигуряването и контрола на разузнаването чрез поставяне на задачи, даване на указания, всестранно осигуряване (правнонормативно, материално-техническо, финансово, кадрово) на службите за сигурност и обществен ред;

г) да осъществява ефективен институционален контрол чрез законодателната, изпълнителната и съдебната власт;

д) да гарантира професионалната автономност в дейността на службите.

4. Укрепване на връзката разузнаване – гражданско общество

Разузнавателните служби подлежат на демократичен контрол от страна на парламента, изпълнителната власт и гражданското общество. Основната цел е службите

за сигурност да бъдат предпазени от политически злоупотреби, без да бъде намалена тяхната ефективност и без да бъдат изолирани от управлението на изпълнителната власт. Службите за сигурност и разузнаване не трябва да се притесняват от опасенията на хората и от желанието им да упражняват контрол чрез техните избрани представители, т.е. избрани цивилни лица в кабинета и парламента, които олицетворяват върховенството на политическия контрол върху службите за сигурност и разузнаване. Накратко демократичният контрол върху службите за сигурност включва редица институции и играчи.

Освен че представлява комплекс от специализирани дейности на институциите, разузнаването е особен социален феномен, защото, от една страна, е негласен инструмент за защита на гражданите, а от друга страна, зависи от отношението, приноса и участието на обществото. Целенасочените усилия за укрепване на доверието на гражданското общество могат в значителна степен да подобрят условията за изпълнение на разузнавателните задачи. За целта от службите за сигурност и обществен ред следва да се очаква:

а) по-често да прибягват до външна експертиза от неправителствени структури, включително от информационно-аналитични и изследователски центрове и академичната общност;

б) ясно да очертават разграничителните линии между функциите на собствена и на чужда територия и конкретно да регламентира ограниченията за действие на собствена територия;

в) да прилагат откритост и прозрачност там, където това е възможно.

Службите по необходимост работят скрито, тъй като характерът на разузнавателните задачи изисква те да бъдат изпълнявани в условия на секретност. Оттук произлиза обстоятелството, което някои възприемат като парадокс, че едно открито демократично общество е защитавано със закрити методи и способи. Други си задават резонния въпрос: Секретност доколко и докъде?

Секретността се „продава“ много лесно, особено сред информационното общество, тя е много интересна и завладяваща. Един от най-съществените въпроси на функционирането на специалните служби е свързан с гаранциите срещу използването на службите за тяснопартийни интереси. В тази сфера постигането на деполитизация е значително по-затруднено, отколкото във въоръжените сили.

Нашата научно-практическа мисъл [2: 116] очертава два подхода към проблема на секретността от позициите на защитата на демократичния принцип на граждански контрол над разузнаването. Първият се основава на разбирането, че секретността е необходима, доколкото служи за скриване на източниците на важна конфиденциална информация. На скриване подлежат и методите, формите, способите, силите и средствата на разузнаването и контраразузнаването.

Вторият подход разглежда секретността като условие, източник и причина за редица провали на гражданския контрол, довели до накърняване на националните интереси или използване на разузнавателна информация за лични или тяснопартийни цели.

В научнотеоретичните изследвания обикновено се стига до извода, че е необходим баланс между секретността и публичността [5]. Някои изследователи са на мнение, че „всяка възможност за увеличаване на публичната информираност за проблемите и операциите на разузнаването извън законно класифицираната информация е от огромна полза за обществото“ [4: 67].

За да прилагат този балансиран подход, службите трябва да имат активна политика за връзки с обществеността, основана на умението им да поддържат необходимия баланс между скритост и публичност. Главен принцип на тази политика е до-

зираната откритост по съществени теми, които засилват връзката на службите с обществото и укрепват институционалния им престиж. Има теми и въпроси, по които службите могат относително свободно да общуват с обществото, например: ролята им в системата на националната сигурност; заслугите им за защита на обществото и държавата; усилията им за постигане на високи резултати и др. Подходът „колкото по-далече от общественото внимание, толкова по-добре“ невинаги е най-удачен, защото капсулира службите и ги изолира от гражданите, които те са призвани да защитават.

Разбира се, за да е успешно това общуване, гражданското общество трябва да е достатъчно зряло, а неговите структури да са добре организирани и независими.

Заключение

Можем да обобщим, че за да се справи с предизвикателствата и проблемите, българското разузнаване и контраразузнаване трябва да прилагат гъвкави и иновативни подходи и непрекъснато да адаптират своите способности към изискванията на средата. Прилагането на разузнавателна политика с ясно очертани приоритети, интегрирана в общата политика за сигурност, ще засили взаимовръзките в триъгълника държавно ръководство – служби за сигурност и обществен ред – гражданско общество и ще допринесе за по-висока ефективност на националния разузнавателен процес.

Технологиите правят много аспекти на шпионажа по-трудни от всякога. В ерата на интелигентните градове, с видеокамери на всяка улица и все по-прилаганата технология за лицево разпознаване, разузнаването стана много по-трудно. За служител на разузнаването, работещ в чужбина във враждебна държава, срещащ се с източници, които рискуват собствената си безопасност, за да предоставят ценна информация, това представлява сериозна заплаха. Но същата технология, независимо дали става дума за добиване на големи масиви данни, за да се разкрият модели в дейностите на чуждите служби, или за широки мрежи от камери, които могат да проследят всяко движение на оперативен агент, може да работи за собствените ни служби и срещу противниците.

В заключение можем да направим обоснован извод, че най-сериозният риск при реализиране на разузнавателна дейност, който може да доведе до повече грешки, отколкото при провеждане на разузнавателни операции, е предубеждението, подценяването и високомерието.

Литература

1. **Ангаров,** Д. Анализ на възможните кризи на фона на глобалните процеси. – В: *Годишник* на ВУСИ, том XXI, 2024. Пловдив: ВУСИ, 2025. ISSN 2367-8798.
2. **Бакалов,** Й. Теоретичен модел на политика за сигурност и граждански контрол на Република България. София: НБУ, 2011. ISBN 978-954-535-689-6.
3. **Стойков,** М. Стратегически преглед на сигурността и отбраната. София: ВА „Г. С. Раковски“, 2019. ISBN 978-619-7478-29-7.
4. **Kniep,** Ronja, et al. Towards democratic intelligence oversight: Limits, practices, struggles. Cambridge University Press, 2023. [online]. *https://www.cambridge.org/core/journals/review-of-international-studies/article/towards-democratic-intelligence-oversight-limits-practices-struggles/9F7573B1EF7EE78F9ED3DE113D753923.*
5. **Landon-Murray,** M. Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate? – In: *Journal* of Strategic Security 8, 2015, No. 3.

РАЗУЗНАВАНЕТО В СЪВРЕМЕННАТА СРЕДА НА СИГУРНОСТ – ПРИОРИТЕТИ, ИЗИСКВАНИЯ, НАСОКИ ЗА УСЪВЪРШЕНСТВАНЕ

ПРЕДИЗВИКАТЕЛСТВА НА СРЕДАТА НА СИГУРНОСТ ПРИ ФОРМИРАНЕ НА РАЗУЗНАВАТЕЛНИ СПОСОБНОСТИ

проф. д.н. Севдалина Димитрова
Висше училище по сигурност и икономика – Пловдив

CHALLENGES OF THE SECURITY ENVIRONMENT IN THE FORMATION OF INTELLIGENCE CAPABILITIES

Prof. Sevdalina Dimitrova, DSc
Higher School of Security and Economics – Plovdiv

Резюме: *Многокомпонентната същност на системата за сигурност в днешната променлива среда на сигурност – динамична, по-често неопределена – пряко е свързана с формирането на разузнавателни способности за страната. В сложната геополитическа и геостратегическа ситуация дискусионен е въпросът за състоянието и приоритетите в разузнавателните структури като част от системата за сигурност, отговорите на който са не само неоднозначни, противоречиви, но и належащи за адекватно противодействие на каквито и да е деструктивни действия, които биха застрашили националните граници и сигурността на гражданите.*

Ключови думи: *сигурност; среда на сигурност; отбрана; разузнаване; способности*

Abstract: *The multi-component nature of the security system in today's changing security environment – dynamic, more often unpredictable – is directly related to the formation of intelligence capabilities for the country. In the complex geopolitical and geostrategic situation, the question of the state and priorities of intelligence structures as part of the security system is debatable, the answers to which are not only ambiguous, contradictory, but also necessary for adequate counteraction to any destructive actions that would threaten national borders and the security of citizens.*

Key words: *security; security environment; defense; intelligence; capabilities*

Предизвикателства на средата на сигурност – вместо увод

Едва ли сме си представяли, че 80 години след края на Втората световна война отново в речника ни и в дискусиите в публичното пространство тази дума „война“ ще заема все по-значимо място. Особено през последните няколко години, от пандемията Covid-19, като че ли глобализацията и неолибералният режим под прикритието на демократически ценности по-скоро се явяват заплаха за световния мир и сигурността в национален, регионален, международен аспект, отколкото предпоставка за неговата стабилност. Проявяващите се във все по-голяма степен отрицателни ефекти са показателни, че световните политически елити и лидери като че ли не са научили поуките от историята и в стремежа за надмощие във всеки един аспект залагат на карта световния мир, бъдещето на човечеството и неговото оцеляване. Особено това важи през последните два месеца за държавите – членки на ЕС, и като цяло за оцеляването на Стария континент – Европа, където ежедневно сме свидетели на все по-неадекватно поведение на предизвикателствата на средата на сигурност, белязана от многокомпонентни кризи, провокиращи непредсказуеми рискове и заплахи за сигурността. Нещо повече, милитаристичните нагласи на европейските лидери, стремежът към псевдолидерска доминация, налагането на „ценности“, нямащи нищо общо с националните в културен, народопсихологически, нравствен аспект, провеждане на политика на санкции, задушаваща икономиките на държавите, превръща ЕС от съюз за икономическо, социално, културно сътрудничество и взаимопомощ в политическо-военен съюз. И

всичко това на фона на задълбочаваща се икономическа криза, водеща до вчера лидерите в икономическо отношение до рецесии, терористични действия на мигранти, превземащи цели райони в Централна и Западна Европа, настъпление на ислямския фундаментализъм, газова и енергийна криза, редица регионални конфликти в Азия и в Северна Африка, в Черноморския регион. Нестабилността и противоречивата политика и на Западните Балкани са не по-малък фактор за пренебрегване, имащ пряко отражение на средата на сигурност в регионален аспект.

В контекста на целия този спектър, определящ динамично променливата среда на сигурност, не е за подценяване и политическата нестабилност, създадените властови зависимости и корупционни практики на всички нива на управление, които не по-малко се явяват заплаха за националната сигурност. Паралелно с това затвърждаващият се ресурсен дефицит и лишена от логика и прозрачност бюджетна технология, дългова зависимост, неаргументирани политики и програми във всички сфери на обществения живот са сериозна предпоставка за кризи от различен характер.

В ретроспекцията на външната и вътрешната среда на сигурност в публичното пространство все по-често дискусионен е въпросът в състояние ли е политиката за сигурност „да създаде необходимите условия и предпоставки за гарантиране на правата на човека и националните интереси, ограничаване на въздействието на рисковете и заплахите, оптимално разпределение на ресурсите и повишаване на сигурността на гражданите“ [1: 13] и в достатъчна степен ли са способностите за адекватен отговор на промените на средата на сигурност.

В търсенето на отговор от позициите на широкоспектърното съдържание на системата за национална сигурност на преден план извеждаме един от нейните компоненти, за които сравнително малко се пише и говори в академичните среди поради неговото естество. Става дума за разузнаването и разузнавателните способности за защита на националната сигурност и противодействие на каквито и да е посегателства срещу интересите на страната ни. Това провокира научните ни търсения, ограничени в обхвата на формирането на определена степен способности за разузнавателна и контраразузнавателна дейност в контекста на предизвикателствата на средата на сигурност и бюджетен дефицит, което определя и целта на настоящата публикация. Става дума за образователния компонент на военноразузнавателните способности на тактическо ниво на управление като елемент на отбранителните способности за Целите на способности на ВС.

Ресурси – способности

Изходна база за изследванията в настоящата публикация са законодателната, стратегическата, програмната рамка и редица нормативни документи, регламентиращи сигурността и отбраната на страната ни в евро-атлантически контекст. Говорейки за способности за различните компоненти на системата за национална сигурност, не можем да пренебрегнем зависимостта ресурси – способности и ефектите, които пораждат за националната сигурност. Още повече че в търсенето на баланс между тези два компонента на тази зависимост следва да се прилага мениджърски подход, продиктуван от обстоятелството, че в сектор „Сигурност и отбрана“ се създава публично благо за сметка на бюджета, в който основният приходоизточник е данъчното облагане. А това подсказва и за чувствителността на данъкоплатците към държавните разходи за сигурност и отбрана и поражда противоречие между нарастващите изисквания и ресурсните възможности на страната, детерминирани от „икономическия потенциал, темповете на икономически растеж, номиналния брутен вътрешен продукт

като база за акумулиране на бюджетни приходи и обслужване на държавните разходи“ [2: 6.]. Поради тази причина отговорите по изследваната проблематика ни се дават от управленската теория и практика чрез въпросите „какво?“, „колко?“, „как?“, „кога?“, „къде?“, „кой?“, обединени от контролния въпрос „защо?“, за да знаем какви разузнавателни способности следва да планираме и формираме в интерес на сигурността и Целите на способности, при това с единна система на командване и управление в мирно и военно време.

В съответствие с посоченото формирането на разузнавателни способности следва да е на основата на разумен баланс между заявени намерения и осигурени възможности за Целите на способности. И тук основният отговор, макар и неednозначен, гравитира около способностите на военното разузнаване за изпълнение на ролята, мисиите, целите и задачите на въоръжените сили съобразно нивото на амбиция, чието проявление е в защита на суверенитета и териториалната цялост на страната с всички разполагаеми сили и средства, създадени по чл. 3 от Вашингтонския договор и в условията на активиран чл. 5 от същия договор, съвместно със сили и средства за колективна отбрана.

Говорейки за „способности“ като основно понятие в управленския процес, следва да разбираме способността на една организация чрез притежаваните от нея ресурси (материални, финансови, човешки и др.) да изпълнява определени дейности и да генерира определени ползи. А това означава, че от начина на трансформиране на на ресурсите, за да придобием определени способности, зависи какви резултати можем да очакваме при постигане на организационните цели. Оттук проявлението на тази трансформация е посредством зависимостта ресурси – способности, която е в основата на отбранителните способности на страната, част от които са военноразузнавателните. В потвърждение е дефинирането на отбранителните способности като „…възможност за изпълнение на действие/действия за постигане на определена цел/цели или желан краен резултат при определени условия и в съответствие с приети стандарти. (…) съвкупност от следните императивно неделими компоненти: доктрини, организационна структура, подготовка, материални ресурси, личен състав, командване и управление, инфраструктура, оперативна съвместимост. Всеки структурен елемент на системата за отбрана може да има повече от една способност и всяка способност може да се предоставя от повече от един неин структурен елемент“ [3: 15].

От това следва, че в основата на формирането на разузнавателните отбранителни способности, адекватни на средата на сигурност, е планирането, базирано на способности, при което в зависимост от наличните си способности с отчитането на ресурсните възможности се търси отговор на въпроса какви способности са необходими за изпълнение на ролята, мисиите, Целите на способности и задачите на ВС. Посредством сравнителния анализ се установяват кои способности следва да се доразвият, кои са излишните и за кои има недостиг. На тази основа се определят приоритетите, в съответствие с които се планират постижимите цели на военното разузнаване, съобразени с нивото на амбиции (политически и военни). Това означава, че в тясна връзка с необходимите отбранителни способности се определят структурата и числеността на ВС и видовете способности, детерминирани от ресурсите за сигурност и отбрана, в потвърждение на зависимостта ресурси – способности. Казано по друг начин, това е и първата стъпка при формирането на военноразузнавателните способности за Целите на способности, в съответствие с което се определя и планираният прием за обучение на необходимите разузнавателни специалисти на тактическо ниво на управление.

Обучение и формиране на военноразузнавателни способности на тактическо ниво на управление

Обучението на специалистите за целите на военното разузнаване на тактическо ниво на управление е в пряка връзка със законодателната рамка и съюзните документи, мисията на Националния военен университет „Васил Левски“, мисията на Служба „Военно разузнаване“ като структура на Министерството на отбраната и приоритетите за военното разузнаване, съобразно които се планират необходимите отбранителни военноразузнавателни способности, адаптивни на предизвикателствата на средата на сигурност. И всичко това – в съответствие с държавната политика за сигурност и отбрана, произтичаща от членството на страната ни в евро-атлантическите структури.

Обучението на офицери на тактическо ниво на управление за целите на военното разузнаване е в Национален военен университет „Васил Левски“ по две военни специализации – „Разузнаване“ и „Електронно разузнаване и електронна война“ в образователно-квалификационна степен (ОКС) „бакалавър“ в професионално направление „Военно дело“, военна специалност „Организация и управление на военни формирования на тактическо ниво“. Спецификата в обучението и формирането на военноразузнавателни способности е, че бъдещият офицер на тактическо ниво на управление придобива и ОКС „бакалавър“ по граждански специалности „Национална и регионална сигурност“ – за военна специализация „Разузнаване“, и съответно „Комуникационна техника и технологии“ – за военна специализация „Електронно разузнаване и електронна война“, като двете специалности взаимно се допълват, съпътстват и надграждат. За тази цел обучението е организирано по единен учебен план по двете специалности на модулен принцип и е подчинено на философията за логическа последователност, поетапно усвояване на мениджърски знания и формиране на необходимите компетенции и лидерски качества по зависимостта базова подготовка – съпътстваща подготовка – надграждане на знанията и способностите. В резултат на това в края на всяка учебна година у обучаемите се формират определен набор ключови и функционални компетентности и компетенции.

На това основание обучението по двете специализации за целите на военноразузнавателните способности е на основата на интердисциплинарна подготовка за придобиване на висше образование по военна и гражданска специалност. Обучението е насочено за реализиране на концепцията за оптимално хармонизиране на подготовката на бъдещия офицер с цел получаване на базова компетентност, знания и умения в областта на военното дело, знания за дейността на гражданските, политическите, социално-икономическите структури и системи. При това в хода на обучението следва да се създадат предпоставки за личностно развитие, активно гражданско участие, социално приобщаване и пригодност за реализация в конкурентна среда и в общество на знанието с европейско измерение.

Ключовите компетенции на офицера на тактическо ниво на управление от двете специализации се изразяват в умението да използва ефективно и рационално информационни и комуникационни технологии; да владее общи и професионални комуникативни умения; да ползва чужд език, като при завършването да е сертифициран по стандарт „STANAGE – 6001“ на НАТО най-малко на ниво 2.2.2.2. по четирите елемента за владеене на чужд език и познания по балкански езици; да познава и спазва правилата за здравословен и безопасен труд.

Задължителен елемент от обучението на бъдещите офицери на тактическо ниво на управление с формирани военноразузнавателни способности е да имат интелектуална, нравствена и физическа, професионална и лидерска подготовка и качества

за реализация като офицер в структурите на ВС и БА и Служба „Военно разузнаване“. В резултат на цялостната му подготовка в университета випускникът от двете специализации следва да е с изградени лидерски и положителни морални и волеви качества, с достатъчно знания в областта на военното дело, техническите и обществените науки, позволяващи правилно разбиране на процесите и явленията в съвременното общество, с експертни знания като организатор и експерт в държавните и местните структури на администрацията и органите по сигурността, както и в международните и съюзните органи за колективна сигурност; с изградени умения за управление в различни условия на взвод и рота и приравнените им, които да му позволяват да се усъвършенства в управлението на по-големи войскови формирования; с развити интелектуални и волеви качества и способност за научни изследвания, свързани със сигурността на държавата и местната власт, които да му позволяват надграждане на оперативно и стратегическо ниво на управление, с висока обща култура и комуникативни способности и да решават конкретни задачи по планиране, организиране и ръководене на военноразузнавателната и бойната подготовка на личния състав, да проявява инициативност и творчество в динамично променящи се условия, да участва в национални и многонационални бойни операции и операции, различни от война.

Успоредно с посочените ключови компетенции бъдещите офицери на тактическо ниво на управление от двете специализации следва да придобият и специални компетенции в интерес на военноразузнавателните способности, изразени в генерирането на нови знания и нови способности. Става дума за знания за: правните основи и нормативната уредба във Въоръжените сили; организацията на подразделенията и частите от родовете войски и специални сили на Сухопътните войски и Военноморските сили; основни положения от теорията по организиране и водене на разузнаването и специалните операции в боя и управление на подчинените подразделения/органи; основните положения от теорията по организирането и воденето на HUMINT разузнаването; устройството, тактико-техническите данни, бойното използване, обслужването и съхранението на разузнавателната и специалната техника и апаратура, системите за тяхното управление и контрол, въоръжението и бойните припаси в повереното му подразделение; математическата основа, стандартите за условни знаци, правилата за работа с топографска карта, системите за целеуказване и съвременните способи и средства за получаване на топогеодезически данни; правилата и реда за работа с видовете бойни документи; основните стандартни и щабни процедури, протоколи и стандартизационни документи в НАТО; общите положения от общата тактика и тактиката на рода войска, подготовката и воденето на видовете бойни операции от общовойсковите подразделения; основите по осигуряване на разузнаването; основите на управлението на кризи и разузнаването при участие в операции, различни от война; възможностите и начините на използване на бойните и техническите средства и системи в разузнаването; парашутната материална част и правилата за изпълнение на парашутни скокове и десантиране на товари; овладяването на комуникативни способности в общуването във военната йерархия; боравенето с индивидуалното въоръжение, методите и правилата за водене на стрелба; основните способи за откриване, обезвреждане и унищожаване на мини и импровизирани взривни устройства; средствата и способите за индивидуална защита от ядрени, химически и биологически оръжия, медицинска помощ и противопожарна защита; психологическите и педагогическите концепции за изграждане на екип, проявяване на грижи и изграждане на дух на доверие, високата мотивация и отговорност за изпълнение на задачите; основите на мрежовоцентричните операции; оценката на обстановката по елементи в изводна форма, вземането на решение за действие на подразделението на карта и на мест-

ността в стегната и ясна формулировка, отдаването на бойна заповед и разпореждания; ръководенето на подразделението в хода на бойните действия чрез комуникационна връзка с подчинените си и висшестоящия командир; комуникацията на английски език чрез използване на основна военна терминология при изпълнение на мисии и съвместни учения с войскови единици на НАТО; основите по осигуряване на бойните операции; основите на компютърното симулиране на тактически задачи; интегрираните системи за управление на войските и оръжията; същността, закономерностите и особеностите на военнопедагогическия процес и изискванията на общата методика и частните методики за организиране и провеждане на занятия по видовете подготовки с подчинените; информационните технологии и съответните знания в областта на националната и регионалната сигурност, респ. на комуникационната техника и технологии.

Специфични компетенции за специализация „Електронно разузнаване и електронна война“ освен посочените са и знанията за: основните положения от теорията по организирането и воденето на електронното разузнаване и електронната война; устройството, тактико-техническите данни, бойното използване, обслужването и съхранението на техниката за електронно разузнаване, системите за тяхното управление и контрол, въоръжението и бойните припаси в повереното му подразделение; основите по осигуряване на електронното разузнаване и електронната война; основите на управлението на кризи и електронно разузнаване и електронна война при участие в операции, различни от война; възможностите и начините на използване на бойните и техническите средства и системи в електронното разузнаване и електронната война; овладяването на комуникативни способности в общуването във военната йерархия.

Генерирането на посочените знания са в основата на изграждането на нови способности за завършващите двете военни специализации за целите на военноразузнавателните способности. Сред тях са: моделиране на явленията и процесите, свързани с планиране, организиране и водене на разузнаването или специалните операции, като прилага творчески придобитите знания в своята многостранна дейност; командване на повереното му подразделение с компетентността на естествен лидер; реализиране на изискванията на системата за командване, контрол, комуникации, компютри и разузнаване (C4I); работа с топографска карта със съвременни средства за навигация, целеуказване, изучаване и оценяване на местността; ръководене на процеса на събиране, анализ и докладване на разузнавателната информация, респ. определяне на координатите на разкритите радиоелектронни средства; изпълняване на всички функционални задължения по организиране на електронно разузнаване и електронна война за всяка конкретна оперативна и радиоелектронна обстановка; организиране и управляване на действията на повереното му подразделение/орган при разузнаване или провеждане на специални операции; умение да използва и да управлява техниката, въоръжението и средствата за разузнаване, свръзка и сигнализация, респ. използване на щатните средства за електронно разузнаване и електронна война; успешно адаптиране при промяна на обстановката, работа в екип и осъществяване на непрекъснат контрол и въздействие върху подчинените си; анализиране на данни, факти и процеси за вземане на оптимални решения и справяне в критични моменти; умение за общуване с различните категории военнослужещи и владеене на правилата на служебната комуникация; въвеждане на уставен ред и дисциплина и спазване на военната етика и морал сред подчинените му; прилагане в своята практическа дейност на стандартизационните споразумения на НАТО и съюзните публикации; владеене на английски език в степен, позволяваща водене на разговор на професионални и битови теми, ползване на литература на английски език по изискванията на STANAGE-6001;

ползване на втори чужд език (балкански език) в степен, позволяваща му самостоятелно да развива лексиката на езика, да комуникира и да си служи с необходима литература по специалността; притежаване на основни компютърни умения за разработване на текстообработващи програми и програми за презентации; притежаване на самообладание и съобразителност, решителност, настойчивост и инициативност, воинска чест и достойнство; притежаване на способност за поемане на разумен риск. Придобитите нови способности в областта на разузнаването и контраразузнаването на офицерите на тактическо ниво на управление се допълват и надграждат и със съответните способности, изискуеми от гражданските специалности – „Национална и регионална сигурност“, респ. „Комуникационна техника и технологии“. И всичко това – в съответствие с притежаваните ценностни ориентации и нагласи: лоялност към институцията, в която работят; толерантност, отвореност и уважение към различните позиции и идеи; лична отговорност и уважение към основните свободи и права на човека; междуличностни, социални и граждански компетенции; естетическа, нравствена и здравна култура; готовност и стремеж към учене през целия живот; комуникативни способности; работа в екип в неоднородна среда; проявяване на грижи и изграждане на дух на доверие, висока мотивация и отговорност за изпълнение на задачите; етика на общуване във военната йерархия; приобщаване към идеалите на родолюбието, дълга и честта; уважение към символите на държавата и армията.

При своята реализация офицерите на тактическо ниво на управление от специализациите „Разузнаване“ и „Електронно разузнаване и електронна война“ се утвърждават с придобитите знания и военноразузнавателни способности, като им се създават условия за надграждане на тези знания и способности в оперативно и стратегическо ниво на управление, както и за академично развитие с принос за Целите на способности съобразно промените на средата на сигурност и нейните предизвикателства. И в този контекст в перспектива и в изпълнение на стратегическата цел изграждане на ВС, които да са „модерни, оперативно съвместими, с единна система за командване и управление в мирно време и при кризи и да разполагат с основните приоритетни отбранителни способности, адекватни на рисковете и заплахите“ [4: 13], военното разузнаване следва да придобива нови, специфични способности, позволяващи добиването, анализа и обмена на разузнавателна информация в съответствие с нивото на амбиция и Целите на способности. Предвижданията в тази насока са „нивото на амбиция за военното разузнаване (...) до 2032 година (...) да изгражда и развива способности за единна комуникационна система на разузнаването за обмен на разузнавателна информация на стратегическо, оперативно и тактическо ниво; „Съвместни ефекти“ при провеждане на информационни операции; Стратегически разузнавателен център; информационно осигуряване и разузнавателна поддръжка на Върховното главно командване, щабовете, войските и силите; киберразузнаване; електронно разузнаване; геопространствено разузнаване; разузнаване чрез изображения“ [4: 21].

Прави впечатление, че така предвиденото ниво на амбиция за военното разузнаване с дългосрочен хоризонт е в подкрепа на Целите на способности на НАТО, но имайки под внимание динамично променливата среда на сигурност с все по непредсказуеми рискове и подготовката на ЕС за война, под въпрос остава реалната изпълнимост поради ресурсни ограничения. Това обстоятелство е предпоставка за разработването на нова стратегия за национална сигурност, с приоритетни и изпълними секторни политики, сред които формирането на разузнавателни способности на страната да е обвързано с ресурсните възможности на данъкоплатците и с реалните заплахи и рискове за сигурността на страната.

Заключение

В обобщение, неоспорим факт е, че живеем в смутно време с непредсказуеми рискове и заплахи не само за националната, но и за регионалната и международната сигурност. Сега, когато сме на прага на прехода от еднополюсен към многополюсен свят, когато се правят опити за налагане на мир и прекратяване на военните действия в отделни райони, Старата Европа се готви за война. Средата на сигурност е все по-динамична и неопределена, рисковете все по-непредсказуеми, а оттук предизвикателствата, перспективите пред разузнаването и контраразузнаването – все по-големи, в контекста на формирането на нови разузнавателни способности както по отношение на глобалните и регионалните рискове и заплахи за страната ни, така и по отношение на многопластовите кризи, асиметричните и хибридните заплахи, миграцията, международното сътрудничество, военното дело. А това само по себе си е предпоставка за далновидност на държавната политика в областта на разузнаването и контраразузнаването, изграждане на необходимите разузнавателни и военноразузнавателни способности за външната и вътрешната сигурност, за което има капацитет и потенциал, съобразно средата на сигурност, дигитализацията на обществените процеси и ресурсната ограниченост на принципа на икономично, ефективно и ефикасно разходване на публичните ресурси.

Литература

1. **Актуализирана** стратегия за национална сигурност на Република България. Приета с Решение на НС от 14.03.2018 г. Обн. *ДВ,* бр. 26 от 23.03.2018 г.
2. **Димитрова,** С. Системи за управление на ресурси за сигурност и отбрана. Велико Търново: Фабер, 2024.
3. **Национална** отбранителна стратегия. Приета с Решение № 131 от 6.03.2025 г. на МС на Република България. [онлайн]. *https://www.mod.bg/bg/doc/strategicheski/20250324_Natsioanalna_otbranitelna_strategia_RMS_131_06.03.2025.pdf.*
4. **Програма** за развитие на отбранителните способности на Въоръжените сили на Република България, 2032. Приета с Решение на Народното събрание от 11.02.2021 г. Обн. *ДВ,* бр. 13 от 16.02.2021 г.

ДИПЛОМАЦИЯ И РАЗУЗНАВАНЕ В СЪВРЕМЕННИТЕ МЕЖДУНАРОДНИ ОТНОШЕНИЯ

проф. д.и.н. Нина Дюлгерова
Висше училище по сигурност и икономика – Пловдив

DIPLOMACY AND INTELLIGENCE IN CONTEMPORARY INTERNATIONAL RELATIONS

Prof. Nina Dyulgerova, DHS
Higher School of Security and Economics – Plovdiv

Резюме: *Основният акцент в доклада е поставен върху трансформацията, която се извършва в установените в исторически план системи на дипломатическа служба и протокол и разузнавателната дейност, преминаваща през динамично променящите се глобални и регионални политически и икономически структури в съвременния свят.*
Ключови думи: *дипломация; разузнаване; геополитически модел; трансформация*

Abstract: *The main emphasis in the article is placed on the transformation taking place in historically established systems of diplomatic service and protocol and intelligence activity, passing through the dynamically changing global and regional political and economic structures in the modern world.*
Key words: *diplomacy; intelligence; geopolitical model; transformation*

Съвременният свят е своеобразна еманация на многовековните процеси, които са достигнали кулминацията си на развитие. След края на Римската империя през V в. устойчивият геополитически модел се развива през имперските политики за власт чрез конфликти и войни. Техният ефективен политически инструмент за контрол чрез сътрудничество и конфронтация са религията, етносът и идеологията. Технологичната революция през настоящия век все още е в процес на утвърждаване на геополитическата космополитна система. Все по-ясно се очертава широкият спектър на ресурси, чието отсъствие или наличие в различни държави и империи предопределя политическите съюзи, икономическите конкуренти и засилващата се тенденция към безнаказано нарушаване на правилата и принципите на международното право. Пандемията от коронавирус, както и украинският казус и войната в Газа, са факторите, които сериозно дестабилизират света. Все още участниците в съвременната международна система продължават да съществуват в контекста на познатите международноправни субекти – държави, международни организации и институции. Същността на международните отношения продължава да се проявява в политиката, провеждана във всички области на обществения живот. Развитието в двустранен или многостранен план на постигнатите споразумения и договори в резултат на преговори в различен формат определят развитието на всяка една сфера в национален, регионален и глобален план. Тези основни за съществуването на всяка институция, организация и политическа единица дейности през вековете са неизменно свързани с два основни фактора – дипломацията и разузнаването. Огромно количество изследвания са проведени относно мястото и ролята на тези две системи в развитието, утвърждаването и разширяването на всяка една държава през вековете. През последните столетия промяната на геополитическите граници на регионално и глобално ниво неизменно е свързана със сложните и динамични отношения между империите. През XIX, XX и

XXI в. междудържавните отношения продължават да преминават през дихотомията мир – война. Процесите на национална идентификация, които определят акцентите на европейската картина преди два века, през следващите десетилетия са в плен на идеологическо противопоставяне. През последния четвърт век се наблюдава засилваща се тенденция за поемане на управлението на човечеството чрез познатия спектър на средства – войни, дипломация, разузнаване, пропаганда и активно използване на високите технологии.

Дипломацията и разузнаването са основните фактори, гарантиращи устойчиво развитие на всяка империя, държава, организация и военна структура. Дипломацията е институция, чрез която се осъществява външната политика. Предполага се, че защитава националните интереси и ако има възможности, осъществява независима политика. Това е сложен процес, който преминава през утвърдена система, в която дипломатическата служба и протокол са неизменни. Разузнаването също е част от общественото развитие. Системата за сигурност на всяка една национална, регионална или глобална институция залага както на добра и навременна информираност, така и на дипломатическите средства, гарантиращи сигурност, стабилност и развитие.

80-те години след края на Втората световна война преминават през биполярното противопоставяне Изток – Запад, с което се характеризира последният етап по пътя към глобализацията. Идеологическото противопоставяне удобно разделя света на два свята, чиято конкуренция се основава на европейската многовекторна разузнавателна дейност, дипломатически преговори и опити за елиминиране.

Този период е известен като „Студена война“, която започва през 1946 г. Все още е актуална тезата, че с разпадането на Източния блок и суперсилата Съветски съюз се поставя краят този глобален сблъсък. Факт е, че с разрушаването на политическата система, създадена след Втората световна война, Студената война не свършва. Част от световните разделителни лагери са още два сегмента – Западният блок, ръководен от САЩ, и Третият свят, който обхваща Азия, Африка и Латинска Америка. Последното десетилетие на XX в. преминава през интересен за човешкото развитие период. Отсъстват врагът, противникът и идеологията, които да координират общественото развитие. Десет години победилите САЩ и Западният свят усилено и многопластово разрушават конкурентния Изток чрез утвърждаване на демокрацията и пазарната икономика в бившите социалистически държави. Последователно и методично се разрушават институции, индустрия, образование, здравеопазване, но най-вече службите за сигурност и армията. Източноевропейските държави вече са част от Европейския съюз и НАТО. Европа вече е обединена. До втория мандат на Доналд Тръмп като президент на САЩ тя се развива като част от евро-атлантическата зона под американско влияние и контрол. Европейската система на проектно финансиране създава удобни условия за разрушаване на икономиката, селското стопанство, здравеопазването и образованието. Корупционната схема преминава през стъкмистика на документацията и отсъствие на устойчиви гаранции за развитие.

В съвременния свят международните отношения в ЕС и НАТО се развиват под знака на безпрекословно подчинение и намаляващи възможности за отстояване и защита на националните интереси и суверенитет. Характерен пример е поведението на българския европреговарящ Меглена Кунева, чийто прякор е „Yes Sir!“. Този модел е устойчиво еднозначен за източноевропейските държави до първите години на XXI в. В продължение на едно десетилетие Руската федерация (наследникът на СССР) преминава през разрушителния процес, кадрово подготвен и организиран от Михаил Горбачов и неговия наследник Борис Елцин. С идването през 2000 г. на власт на Владимир Путин Русия започва постепенно да се възстановява. Енергийният XXI в. в контекста на неизчерпаемите находища на конвенционални суровини (нефт и газ) създава

благоприятни условия за развитието на бившата суперсила. През следващите години засилващата се зависимост от електроенергия предопределя до голяма степен акцентите и поведението на политици и дипломати най-вече в Европа. До 2014 г., когато се осъществява държавният преврат в Украйна, международните отношения преминават под знака на икономическата надпревара, политическото лобиране и т.нар. „цветни революции“ в постсъветското пространство. Активно осъществяваната от Москва геоенергийна стратегия за изграждането на южна и северна тангента от газопроводи към Европа се превърна в основен елемент от дипломатическата дейност на двустранните и многостранни инициативи и действия в триъгълника ЕС – Русия – САЩ. Засилващите се взаимноизгодни енергийни отношения между европейските политици и дипломати с транснационални руски компании, като „Роснефт“, „Газпром“ и „Росатом“, определят акцентите на международния дневен ред. Строящите се енергийни проекти, като газопровода „Южен поток“, „Северен поток 1 и 2“ в южна и северна посока, не само възстановяват икономически Русия, но и предизвикват негативните реакции на транснационалните американски компании. Те губят не само огромни печалби, но и политически възможности за контрол върху европейските политици и институции. Съществен елемент от войната за изтласкване на Русия от европейския енергиен пазар е влезлият в сила през 2011 г. Трети енергиен пакет. В него категорично е записано, че построените конвенционални транзитни коридори трябва да се използват не само от руските газови и нефтени компании, но и от други търговци на тези суровини [6].

Енергийната сигурност се превръща в основен елемент от дипломатическата и разузнавателната дейност на европейските държави, Русия и САЩ. В контекста на този процес през 2009 г. американският президент Барак Обама обяви основния външнополитически приоритет на Вашингтон – шистова дипломация. България, Румъния, Украйна и Полша в продължение на няколко години бяха обект на проучване за шистов газ, чиито резултати с оглед на прилаганата опасна технология имат своите негативни в екологичен план последствия. Неуспехът на американската геоенергийна политика преструктурира външната политика на Вашингтон.

Моделът се трансформира вече в познатата от векове схема преврат – разрушаване – нестабилност. През първите години на второто десетилетие на XXI в. отново се направи опит да се дестабилизират три основни фактора в постсъветското пространство – Грузия, Киргизстан и Украйна. През 2008 г. Тбилиси загуби в Кавказката война контрола върху Абхазия и Южна Осетия, но през 2014 г. след падането от власт на Михаил Саахашвили Вашингтон загуби съществено своето влияние в Грузия. Киргизстан през 2010 г. съумява да завърши започналата 5 години преди това половинчата „революция на лалетата“, чрез която се установява достатъчно устойчив политически режим в страната.

Имайки предвид стратегическото геополитическо разположение на Украйна, тя се превръща в основен коз на англосаксонските политически и военни структури за отслабването и разрушаването на Руската федерация. Евромайданът, организиран и финансиран от САЩ, независимо от многобройните срещи и преговори между европейските и украинските политици през февруари 2014 г. води до сваляне от власт на легитимно избрания президент Виктор Янукович, който е принуден да избяга в Русия. Неслучайно тогавашният зам.-държавен секретар Виктория Нюланд заявява, че „вложените 5 млрд. долара са гаранция за демократичните промени в държавата“ [7]. С преврата в Украйна се поставя началото на динамични опити за преструктуриране на евразийското пространство, вкарвайки Русия и Европа в разрушителната парадигма на дипломацията, пропагандата, както и на финансовото и военното разрушаване на ЕС и НАТО.

През последните десетина години международните отношения вече имат нова съдържателна характеристика. Сигурността продължава да се гарантира чрез дипломатическите и разузнавателните средства, познати от миналото. Западноевропейският елит отново прилага позната схема от годините преди избухването на Втората световна война. Постепенното изграждане на политическата доктрина и система на Третия райх преминава през активните дипломатически преговори, сложни схеми и мобилни съюзи. Крайният резултат е обявената от нацистка Германия война на СССР, чрез която за пореден път се прави опит да бъде разрушена и разграбена Русия.

Този модел отново се прилага при украинския казус. През периода 2014 – 2022 г. политическият и дипломатическият формат на преговорите преминава през контактна група (Русия, Украйна и Организацията за сигурност и сътрудничество в Европа), работеща по Минските споразумения от 2014 – 2015 г., както и през преговорния процес на Нормандската четворка (Франция, Германия, Русия и Украйна). През 2015 – 2016 г. демонстрираната от Запада дипломатическа активност за пореден път доказа, че целта не е решаването на украинския въпрос. Войната, която Киев започва срещу жителите на Донецка и Луганска област, води до огромни жертви сред цивилното население“ [5]. Този геноцид не притеснява лидерите на Германия и Франция. Доказателство за това са думите на германския канцлер Ангела Меркел няколко години покъсно. Тя признава, че „протакането на преговорите е с цел да се даде време на Украйна да стане по-силна“ [4].

Украйна се превърна не само в инструмент за отслабването и разрушаването на Русия, но и опит за сериозна геостратегическа победа на Запада. С референдум, проведен на 16.03.2014 г. сред населението на Кримския полуостров, той е върнат в границите на Руската федерация. Факт е, че през следващото десетилетие западноевропейската и американската реакция по този въпрос се ограничи в рамките на моралната риторика на техните политици и дипломати. Не се правят опити за промяна на установеното от март 2014 г. геополитическо статукво.

До 24.02.2022 г., когато Русия започва своята специална военна операция, в международен план дипломацията и разузнаването на държавите от Европейския съюз и НАТО работят за политическа и военна консолидация срещу постоянния враг – Русия.

Пандемията от коронавирус, чрез която светът премина през генералната репетиция за глобално подчинение, също създаде подходяща ситуация за поемане по пътя към глобализацията. От началото на световната пандемия светът започна бързо да се променя. Трансформацията е подчинена на дихотомията мир – война, но известните и устойчиви през последните векове правила търпят драстична промяна. Администрацията на американския президент Джо Байдън поведе войната срещу Русия чрез познатите средства на пропагандата, както и със саморазрушителната политика на даване на военна техника и милиарди евро и долари на Украйна. Тази политика е потвърждение на известната фраза на Збигнев Бжежински от книгата му „Голямата шахматна дъска“ от началото на 90-те години на XX в., че „Украйна е инструментът за разрушаването на Русия, православието и Европа“ [1: 125].

За пореден път Западът не успява в своите планове. Дипломацията отново показва зависимост, неадекватност и разрушителна за европейските общности действия. Резултатите са негативни за Стария континент.

Във военнотехнически и разузнавателен план ситуацията също се трансформира. Технологиите вече са съществена част от войната. Битката на бойното поле остава, но оперативната информация от сателитите, дроновете и снарядите с далечен обсег на действие вече се превръща в основен елемент за победа или поражение. Много явно това проличава през краткия период, през който американският президент

Доналд Тръмп забранява на украинското разузнаване и военно командване да използват американски сателити.

В украинския казус се прилага и един нов момент, който е в унисон с известната фраза на германския министър от Третия райх Гьобелс, че една лъжа, повторена сто пъти, се превръща в истина [2]. През последните 3 години на военни действия политици и дипломати утвърждават тезата за победителката Украйна, за която с всестранната помощ на обединена Европа е въпрос на време да победи. Освен това русофобията целенасочено се налага като основен елемент от образователната система, медиите и социалните мрежи. През десетилетията западната пропаганда, първоначално в политическата система на Запада, утвърждава тезата за изостанала Русия и минималното ѝ участие във Втората световна война, в която единствени победители са САЩ и Великобритания. Нямат значение военните победи на Червената армия и фактът, че тя първа влиза в Берлин и развява знамето на победата над Райхстага.

Половинвековното идеологическо противопоставяне през втората половина на XX в. формира поколения в Източна Европа, възпитавани чрез документи, изследвания и уроци по история, където фактологията убедително разкрива театъра на военните действия в Европа и по света. През неолиберална период на обществено развитие в глобален план, в който унифицираната образователна система в цяла Европа е подчинена на формулата „Западът винаги е победител“, се формират поколения, при които функционалната неграмотност и липсата на основополагаща база знания и духовност са в унисон със засилващата се тенденция към неграмотност, агресия и нежелание за усвояване на нови знания.

Създаването на организиран хаос в политическото пространство и социалните мрежи е съзнателно организиран процес, който позволява лесно, удобно и безнаказано да се утвърждават удобни за глобалното англосаксонско и ционистко задкулисие обществени модели. В тях сигурността като гаранция за съществуването на държава, съюз или организация вече не се нуждае, както в миналото, от традиционните дипломатически и разузнавателни средства. Необятното виртуално пространство, както и новите технологии и засилващите се възможности на изкуствения интелект създават непознати досега възможности за формулиране или утвърждаване на удобни за европейските и англосаксонските институции модели. Изграждането на демоничния образ на тиранина Владимир Путин и на невинната жертва Володимир Зеленски вече е част от виртуалния процес, придружен с познатите форми на дезинформация и морална дидактика.

Интересен момент от този процес е случаят с интерпретациите на неолибералната преса и политическата реакция на западноевропейския елит след смъртта на руския дисидент Алексей Навални през февруари 2024 г. в руски наказателен лагер. Реакцията на дисидентите в Русия и в Европа, подкрепени от неолибералите в ЕС, не приемат позицията на Москва, отричаща съпричастност към смъртта на Навални. Дискусията приключва, когато ръководителят на украинското разузнаване съобщава, че смъртта на руския дисидент е причинена от тромб [3].

През последните две години геополитическият модел, в който дипломацията и разузнаването са основни компоненти на международните отношения, преминава на следващ етап на развитие. Ситуацията се усложнява с нападението на терористичната организация „Хамас“ в Израел и нахлуването на украински военни части в Курска област. И двата военни акта са неочаквани за Тел Авив и за Москва. Изтъкват се многобройни причини за тези фрапиращи със своята ефективност действия. Израелският премиер Нетаняху започна широкомащабна военна операция срещу палестинското население в Ивицата Газа, а Кремъл осъществи сериозни кадрови промени във

Военното министерство. Международната система коренно се промени и след началото на втория мандат на Доналд Тръмп, чиято инаугурация се състоя на 20.01.2025 г. Новата администрация съзнателно и целенасочено постави на сериозно изпитание принципите на международното право. Още първите заявления и подписани укази на президента Тръмп върнаха света в XIX в. Обявената търговска война към почти всички държави по света, както и безапелационните заявки за присъединяване на Гренландия към САЩ, както и превръщането на Канада в 51. щат, са заявка за световно господство без доказано реално силово икономическо и военно присъствие в глобален план. Вярно е, че тандемът Тръмп – Ванс е представител на индустриалния и технологичния капитал на САЩ, чиято задача е да неутрализира негативните резултати от управлението на Байдън – Харис. Новият президентски дует работи на принципа „доброто и лошото ченге“, а Тръмп действа като бизнесмен. Финансовото и икономическото възстановяване на Щатите изисква елиминиране на конкуренцията в регионален и глобален план. Неслучайно американският президент често заявява, че не би допуснал войната в Украйна. Коренна промяна се наблюдава и в политиката на Вашингтон към Европа. Изоставена Европа е с намаляващи икономически възможности, отсъствие на модерна военна техника и добре обучени военни части. Впечатляваща е активността на „коалицията на желаещите“, чиито инициатори са Лондон и Париж. Неистовото желание на европейския Запад за безусловна подкрепа на Украйна в нейната битка срещу Русия е част от политиката за институционално оцеляване, което е далеч от реалността. Тя е неизменно свързана с плановете на американската Демократическа партия, търсеща в Европа политически реванш след загубените президентски избори през ноември 2024 г.

Създава се интересна ситуация. ЕС и НАТО продължават регламентираната и осъществявана от администрацията на Байдън политика в подкрепа на режима на Киев. Тръмп води открит диалог с Путин и Зеленски за прекратяване на войната. Продължава разрушителната за европейските общества политика на икономически санкции срещу Русия и експулсирането на руски дипломати. От друга страна Вашингтон и Москва постигат споразумение за възстановяване на дипломатическите си представителства.

Паралелно с украинския казус много интензивно се развиват събитията в Близкия изток. Впечатляващи са разрушителните действия на Израел в Ивицата Газа, Южен Ливан и Сирия. За пореден път се надграждат процеси, чието начало има близо 80-годишна давност. Официален Тел Авив постоянно повтаря, че битката срещу „Хамас“ преминава през етническото прочистване на Ивицата Газа. Той получава безапелационната подкрепа на президента Тръмп, който заяви, че тази територия може да се превърне в Ривиерата на Близкия изток [8]. Искането за освобождаването на израелските заложници се превръща в основен мотив за многочислените жертви цивилни палестинци, чийто брой надхвърля 50 000 души. Впечатляващи са и наземните и въздушните удари в Южен Ливан и Източна Сирия. Унищожаването на прокситата на терористичната организация „Хизбула“, подкрепяна от дългогодишния враг на Израел и САЩ – Иран, е в официалната програма на Тел Авив. Нов момент в активните военни действия на Нетаняху в региона е отпадналата необходимост от разузнавателна дейност, когато става въпрос за обстрелване със снаряди. Предупреждаването на институциите и населението в региона за артилерийски обстрел се превръща в устойчива практика.

В съвременния свят на технологиите и активните опити за преминаване на човечеството към друга форма на управление все още са актуални спорадичните прояви на дипломатически преговори и споразумения. Глобалните и регионалните процеси са многовекторни и показват много ясно как се променя етимологията на нападател –

жертва. В украинския казус Киев изтезава и убива многобройни цивилни в Курска област и Донбас с активната подкрепа на западноевропейски наемници и инструктори, за което никой не споменава. Огромната корупция и безследно изчезналите милиарди и получена военна техника са основна част от действията на киевския режим. Нещо подобно се случва и с осъществяваната от Тел Авив политика на геноцид спрямо палестинското население в Ивицата Газа.

Дипломацията и разузнаването в съвременните международни отношения все повече губят своето значение като съществен елемент от запазването и отстояването на държавността. Международноправните принципи съществуват, но постепенно губят своето значение при формулирането и осъществяването на външнополитически цели. Светът е в преход, когато за пореден път на преден план излиза прилагането на универсалния принцип „правото на силата“.

Литература

1. **Бжежински,** З. Голямата шахматна дъска. София: Обсидиан, 1997, с. 125.
2. **Йозеф** Гьобелс. [онлайн]. [прегледан 2.05.2025]. *https://bg.wikiquote.org/wiki/Йозеф_Гьобелс.*
3. **Шефът** на украинското разузнаване: Навални е починал от тромб. – В: *Bulgaria ON AIR,* 26.02.2024. [прегледан 7.05.2025]. *https://www.bgonair.bg/a/4-world/336358-shefat-na-ukrainskoto-razuznavane-navalni-e-pochinal-ot-tromb.*
4. **Angela** Merkel. Hatten Sie gedacht, ich komme mit Pferdeschwanz? Interview. – In: *Der* Zeit, Nr. 51, 2022, 7. Dezember 2022. [online]. [verfügbar 8.05.2025]. *https://www.zeit.de/2022/51/angela-merkel-russland-fluechtlingskrise-bundeskanzler/komplettansicht.*
5. **Conflict**-related civilian casualties in Ukraine. United Nations Humans Right. Office of The High Commissioner, 27 January 2022. [online]. [available 2.05.2025]. *https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ukraine.un.org/sites/default/files/2022-02/Conflict-related%2520civilian%2520casualties%2520as%2520of%252031%2520December%252202021%2520%2528rev%252027%2520January%25202022%2529%2520corr%2520EN_0.pdf&ved=2ahUKEwieguPVsa2NAxUxBNsEHeQoLsYQFnoECB4QAQ&usg=AOvVaw1Oc68LXKVXqgKk_dQzpzUE.*
6. **Governance** of the internal energy market. European Commission. Energy, Climate change, Enviroment. [online]. [available 1.05.2025]. *https://energy.ec.europa.eu/topics/markets-and-consumers/governance-internal-energy-market_en.*
7. **Snider,** Ted. The American Conservative, 21.09.2024. [online]. [available 4.05.2025]. *https://www.theamericanconservative.com/the-damage-victoria-nuland-has-done/.*
8. *https://bntnews.bg/news/shokirashto-absurdno-prekaleno-gaza-se-prevrashta-v-rivierata-na-blizkiya-iztok-1325585news.html.* [прегледан 5.05.2025].

АСПЕКТИ НА КОНКУРЕНТНОТО РАЗУЗНАВАНЕ

проф. д.н. Михаил Михайлов
Висше училище по сигурност и икономика – Пловдив

ASPECTS OF COMPETITIVE INTELLIGENCE

Prof. Mihail Mihaylov, DSc
Higher School of Security and Economics – Plovdiv

Резюме: *Недостигът на ресурси, конкурентният дисбаланс, нелоялната конкуренция и цифровата революция създават рискове за всяка бизнес организация. Оцеляват само онези фирми, които осигуряват най-пълно покритие на потребителските изисквания и използват иновативни методи на управление, докато неконкурентоспособните биват изтласкани от пазара. За да получат пълна информация за своя бизнес, отрасъла и пазарните условия, просперициращите фирми използват конкурентно разузнаване в своето управление. Прилагането му от организациите води до организационна стабилност, по-голяма конкурентоспособност и устойчиво развитие на техния бизнес.*

Ключови думи: *конкурентно разузнаване; цикъл на разузнаване Аштън – Стейси*

Abstract: *Resource scarcity, competitive imbalances, unfair competition and the digital revolution create risks for any business organization. Only those firms that provide the most comprehensive coverage of consumer demands and use innovative management methods survive, while the uncompetitive are driven out of the market. In order to obtain complete information about their business, the industry and market conditions, prosperous firms use competitive intelligence in their management. Its implementation by organizations leads to organizational stability, greater competitiveness and sustainable development of their business.*

Key words: *competitive intelligence; Ashton-Stacy intelligence cycle*

Съвременния свят е в състояние на дълбоки трансформации. Недостигът на ресурси, пазарните дисбаланси, нелоялната конкуренция и дигиталната революция създават рискове за всяка бизнес организация. Във време на големи политически и икономически промени оцеляват само тези фирми, които осигуряват най-обхватно потребителските изисквания и ползват иновативни методи в управлението си, а неконкурентоспособните биват изтласквани от пазара. За да получат пълна информация за бизнеса си, за отрасъла и пазарната конюнктура, просперициращите фирми ползват в управлението си конкурентно разузнаване.

Генезис и еволюция на конкурентното разузнаване

Разузнаването е съпътствало човешкото развитие. Според Тодор Бояджиев [1: 13] разузнаването е втората най-стара професия. За К. Георгиев разузнаването е първата професия, защото Юда в „Тайната вечеря“ е информатор, който е вербуван за 30 сребърника [3: 33].

През аграрния период разузнавателната дейност е хаотична и е свързана предимно с лова и опасността от дивите животни. Във времето до Индустриалната революция разузнаването се легитимира като дейност, свързана с формирането на държавата.

Първият оцелял до наши дни трактат „Изкуството на войната“ на военния стратег Сун Дзъ (живял около 500 г. пр.н.е.) се изучава и до днес както от военни, така и от управленци в различни области на обществото. Този знаменит труд не е загубил

актуалността си през хилядолетията. В него Сун Дзъ пише: „Ще победи този, който знае кога да се сражава и кога не“. Вместо война Сун Дзъ се насочва към други алтернативи, като очертава различни стратегии, като: „Когато можеш да нападнеш, трябва да изглежда, че не можеш“, или: „Когато си близо, трябва да внушаваш на врага, че си далече“. Много съвременно за всяко управление звучат изводите му: „Ако ти познаваш себе си и противника, не трябва да се страхуваш от изхода на сто битки. Ако ти познаваш себе си, но не и противника, за всяка спечелена битка ти ще понесеш по една загуба. Ако ти не познаваш противника, нито себе си, ти ще претърпиш поражение във всяка битка“ [9]. Тези напътствия са приложими както за военната, така и за управленската философия и конкурентната борба между стопанските организации. Бизнесът също е битка, но за разлика от войната той намира израз в съревнованието.

В книгата на Дейвид Браун „Изкуството на бизнес войните“ всяка глава е свързана тематично с някоя от главите в „Изкуството на войната“. Следвайки гения Сун Дзъ, Браун доказва, че в конкурентната борба успяват компаниите с интелект, стратегия и ресурси [2].

В Древна Гърция, Египет и Рим разузнаването се променя. Появяват се тайни сътрудници, които подпомагат търговците. Първата близка до съвременното разузнаване система, опираща се на голяма шпионска мрежа, е на Марк Лиций [10], който е сътрудник на Гай Юлий Цезар.

През Средновековието се утвърждава ролята на разузнаването като фактор за военно и икономическо развитие на обществата. Китайските императори ползват разузнавателни методи за защита на доминацията на Китай на световния пазар на коприна и порцелан.

За Йордан Начев създател на икономическото разузнаване е Чингис хан (ок. 1162 – 1227 г.) – хан на монголите и основател на Монголската империя. Преди всяко нашествие той проучва икономическото състояние, природните богатства и стопанството на териториите, които смята да завладее [5].

Първата частна финансово-икономическа служба, която е свързана с разузнавателна дейност, е създадена от банкерите във Флоренция през XIV век. По-късно този тип дейност намира последователи сред изявени финансисти и банкери, като Ротшилд [6].

Според Боян Чуков съвременното разузнаване се ражда като организация в Рим при Светия престол от Джовани Ботеро (1544 – 1617). Той пръв осъзнава „феномена на институционализиране на информационно-аналитичната дейност в полза на националния интерес“. Ботеро изготвя първия геополитически справочник „Relazioni Universali“, в който очертава „публичната мощ на държавите: военна сила, икономическо, демографско, културно състояние“ [11: 53].

В периода на Великите географски открития (XV – XVIII век) и установяването на държавата като основен политически субект (Холандия, Испания, Португалия, Англия) те водят сериозна икономическа борба с цел завладяване на новооткрити територии и пазари. През този период основното внимание на разузнаването пада върху търсенето, намирането, замяната на суровини и материали.

Краят на XIX век бележи стартирането на маркетингови проучвания в САЩ. Техните резултати служат за анализ на конкурентните фирми в отрасъла.

По време на Втората световна война паралелно с военното разузнаване се засилва и икономическото, като събраната от него информация се превръща в основа за преразпределение на световния пазар след войната.

През периода 1945 – 1990 г. българското икономическо разузнаване е насочено към научно-техническата област и към високоразвитите индустриални държави. 14

000 сътрудници разузнават биотехнологии, роботика, приборостроене, микроелектроника, дискови устройства и ноу-хау технологии. Те допринасят за намаляване на технологичната разлика между България и западните държави [4: 16 – 17].

От 80-те години на XX век конкурентното разузнаване е в подем. През 1985 г. Ленърд Фълд публикува „Разузнаването на конкурента“, а през 1986 г. е основана първата Организация на професионалистите по конкурентно и стратегическо разузнаване, която до края на века събира хиляди членове. Понастоящем конкурентното разузнаване е средство за подобряване на конкурентоспособността на фирмите.

Същностни аспекти на конкурентното разузнаване

Понятийният апарат е в основата на всяка наука. Понятията и терминологията са база и елементи, които дават представа за всяка дейност.

Думата „разузнаване“ („intelligence“) има латински произход и се състои от две думи „inter“ („между“) и „legade“ („събирам“), като, когато се обединят думите, те означават „широк обхват на събиране“ [3: 56].

В Речник на българския език „разузнаване“ е дума от среден род и означава „специална служба, която разузнава“ [7].

В Dumite (Речник на българския език) значението на думата „разузнаване“ е „специална дейност, която има за цел събиране и обработка на информация за даден обект или противник“ [8].

Синоними на разузнаването са: изследване, разследване, изпитване, проучване, проверяване и др.

Значението на думата „конкуренция“ в Речник на българския език е: „1. Надпревара между производители, търговци за пласиране и продаване на стоката при най-изгодни условия. 2. Борба между съперници, които се стремят към едно и също постижение“ [7].

В литературата определенията на „конкурентно разузнаване“ са десетки.

Приема се, че конкурентното разузнаване е етичен и съобразен със законите мониторинг на средата и конкурентите, чиято цел е вземане на стратегическо решение за успешното развитие на организацията (продукт, пазар, цени, потребители, технологии и др.).

За разлика от конкурентното разузнаване, промишленият шпионаж е незаконно събиране на технически решения, крадене на ноу-хау (патенти, технологии, иновации), незаконно подслушване, саботаж на производства и информационни системи. Целите на промишления шпионаж са осъществяване на предимство пред конкурента и материална изгода. Извършващите промишлен шпионаж носят наказателна отговорност по:

- Наказателния кодекс;
- Закона за изменение и допълнение на Наказателния кодекс;
- Закона за специалните разузнавателни средства;
- Закона за защита на конкуренцията;
- Закона за защита на търговската тайна.

Всяка опериращa на пазара организация е изправена пред следните рискове, идващи от:

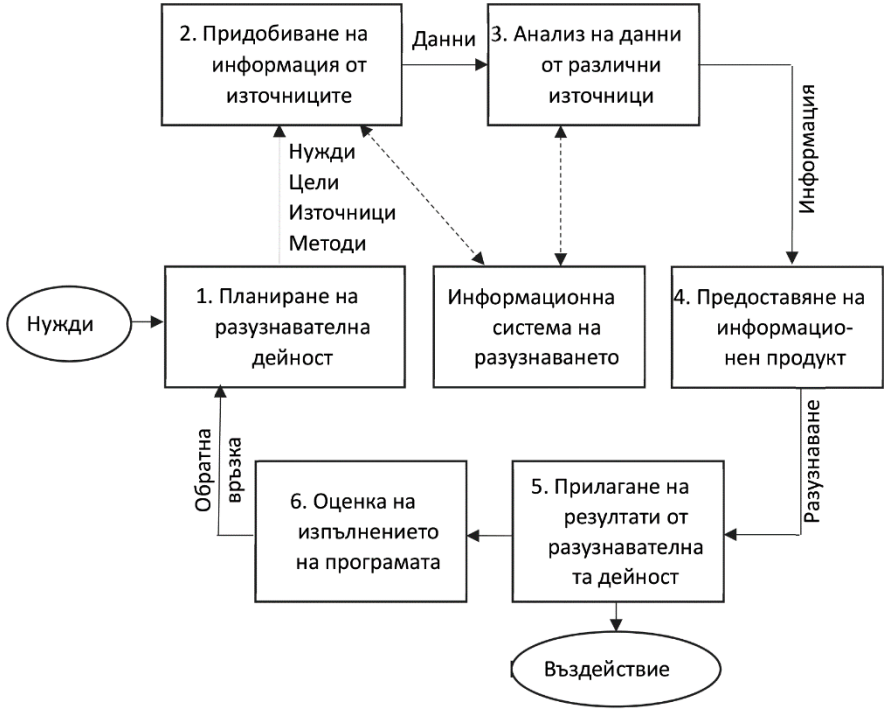
- международната среда;
- социално-икономическата среда;
- технологичната среда;
- политическите процеси;

- законодателната и нормативната среда;
- опазването на конфиденциалната тайна;
- провокациите от страна на конкурентите и др.

За да получат обективни отговори на гореизброените рискове в реално време и за да придобият организационна гъвкавост, фирмите се ориентират към конкурентно разузнаване.

Процесът на конкурентно разузнаване може да се представи с разузнавателния цикъл на Аштън и Стейси *(Фиг. № 1).*

Фигура № 1. ***Разузнавателен цикъл на Ashton & Stacey***



Източник: *Ashton & Stacey [12].*

Мениджърите идентифицират нуждите от разузнавателна информация. На базата на поставените стратегически цели се определят тези нужди и източниците (вътрешните и външните – *Фиг. № 2*), от които трябва да постъпи информация.

Посочват се методите на събиране на информация. След това се планира разузнавателната дейност. В случай, че организацията няма собствена служба за сигурност, се наема външна, специализирана в конкурентното разузнаване организация срещу заплащане. Обичайно целите на разузнавателната дейност са информация за средата и за конкурентните фирми в отрасъла. Тази първа фаза определя успешността на конкурентното разузнаване.

Фигура № 2. ***Източници на информация***

Съставил: *Авторът.*

Втората фаза е свързана с придобиване на информация от източниците, които са заявени. За тази цел се ползват: извличане на данни, текст, патент и други интернет данни. Мениджърите на организациите трябва да осигурят финансово и информационно използване на нови методи за придобиване на информация от източниците. Ползва се специализиран софтуер с данни за бизнеса.

Третата фаза е свързана с анализ на данните и е най-важната в модела на разузнаване. Това е етапът, при който получените данни (статистиките, фактите, графиките и др.) се превръщат в модели, които само много опитни аналитици са в състояние да оценят и интерпретират.

Четвъртата фаза е представяне на резултатите от разузнавателната дейност. Аналитиците докладват на ръководството на организацията получените и анализирани резултати с презентация или доклад.

Петата фаза е завършване на разузнавателния модел (цикъл). Тази фаза е свързана с прилагане на резултатите от разузнавателната дейност. В тази фаза висшето ръководство на бизнес организацията оценява разузнавателния продукт и ако има възражения, дава заявка за нова информация.

Чрез модела (цикъл на Аштън и Стейси) суровата информация се превръща в база за усъвършенстване на управлението на фирмата.

Конкурентното разузнаване е средство за:

- увеличаване на конкурентоспособността;
- повишаване на качеството на продукцията;
- разширяване на пазарния дял;
- подобряване на стратегическото управление;
- изграждане на партньорства;
- подобряване на взаимовръзките със заинтересовани лица;

• увеличаване на иновациите в организацията и др.

В настоящето, когато конфликтността и конфронтацията в бизнеса са повсеместни, а хибридните атаки и конкурентните отношения влияят на бизнес организациите, конкурентното разузнаване е важен инструмент за организационната стабилност. Въвеждането му от фирмите води до по-голяма конкурентоспособност и устойчиво развитие.

Литература

1. **Бояджиев,** Тодор. Разузнаването като занаят. София: Захарий Стоянов, 2002. ISBN 954-739-28-67.
2. **Браун,** Дейвид. Изкуството на бизнес войните. София: Книгомания, 2021. ISBN 978-619-195-301-1.
3. **Великов,** Иво. Кратка история на разузнаването. София: Албатрос, 2017. ISBN 978-954-751-120-0.
4. **Матев,** Николай. Разузнаване, контраразузнаване и вътрешна сигурност на търговската фирма. Велико Търново: Абагар, 2022. ISBN 978-619-168-306-2.
5. **Начев,** Йордан. Вербовка, агентура, разузнаване. София: Труд, 2006. ISBN 954-528-6385.
6. **Начев,** Йордан. Конкурентно разузнаване. София: Сиела, 2007. ISBN 978-954-28-0025-5.
7. **Речник** на българския език. [онлайн]. [посетен 24.03.2025]. *https://rechnik.chitanka.info/.*
8. **Речник** на българския език. [онлайн]. [посетен 24.03.2025]. *https://dumite-bg.com/.*
9. **Сун Дзъ.** Изкуството на войната. София: Хеликон, 2020. ISBN 978-954-298-497-9.
10. **Хюз-Уелсън,** Джон. За разузнаването. История на шпионажа и тайния свят. София: Труд, 2017. ISBN 978-954-398-52-34.
11. **Чуков,** Боян. Разузнаването отвътре – разузнавачи, шпиони и агенти. София: Изток – Запад, 2021. ISBN 978-619-01-0960-0.
12. **Ashton,** W. B., G. Stacey. Technical intelligence in business: understanding technology threats and opportunities. [online]. [available 21.03.2025]. *https://www.semanticscholar.org/paper/Technical-intelligence-in-business%3A-understanding-Ashton-Stacey/fd7c6af7e08eaf13fb15600e2870b0777dd658d1.*

ВЗИМАНЕ НА РЕШЕНИЯ В НАЦИОНАЛНАТА СИГУРНОСТ: СТРАТЕГИЧЕСКО РАЗУЗНАВАНЕ

проф. д-р инж. Максим Алашки
Висше училище по сигурност и икономика – Пловдив

NATIONAL SECURITY DECISION MAKING: STRATEGIC INTELLIGENCE

Prof. Eng. Maxim Alashki, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Представено е т.нар. „разузнавателно общество“ съгласно свързаното национално законодателство, като е развито в подробности стратегическото разузнаване, представено най-вече от аналитичното разузнаване. Темата е обвързана с взимането на стратегически решения от държавното ръководство.*
Ключови думи*: „разузнавателно общество“; стратегическо разузнаване; аналитично разузнаване; стратегически решения; вземане на решения*

Abstract: *The so-called „intelligence society“ is presented, in accordance with the relevant national legislation, and strategic intelligence, represented mainly by analytical intelligence, is developed in details. The topic is related to strategic decision-making by the state leadership.*
Key words: *„intelligence society“; strategic intelligence; analytical intelligence; strategic decisions; decision-making*

Съгласно Закона за управление и функциониране на Системата за защита на националната сигурност Държавна агенция „Национална сигурност“ (ДАНС), Държавна агенция „Разузнаване“ (ДАР) и Служба „Военно разузнаване“ (СлВР) формират т.нар. „разузнавателно общество“ съгласно едноименните закони, а именно Закона за ДАНС, Закона за ДАР и Закона за СлВР, които регламентират техните функции, принципи, права и задължения, както и други специфични въпроси, свързани с тяхната особена дейност. Осъществяваната разузнавателна дейност от тези разузнавателни органи, която наричаме „стратегическо разузнаване“, е свързано с взимането на решения от държавното ръководство в областта на националната сигурност по установен в нормативните документи ред и в рамките на Системата за защита на националната сигурност на Република България [1]. Съгласно професионалната терминология в предметното направление различаваме два вида разузнавателна дейност – аналитично разузнаване и контраразузнаване. Във фокуса на настоящото изложение, свързано с взимането на решения, е стратегическото разузнаване, което е демонстрирано предимно от аналитичното разузнаване, и до голяма степен може да бъде идентифицирано с него. Контраразузнаването е обвързано предимно с дейности по разкриване на чужди разузнавателни органи и преобладаващо на територията на страната ни, то е основно в прерогативите на Държавна агенция „Национална сигурност“ и не е тема на доклада.

Функциите, задачите и дейностите на стратегическото разузнаване се изразяват в изпълняване на задачи, свързани със сигурността и отбраната на страната и защитата на националната и колективната сигурност от посегателства (вътрешни и външни), рискове и заплахи. Разузнавателният цикъл се състои от четири основни дейности и включва дейности по планиране, добиване, обработване и разпространение

на знания (данни, информация) [3]. Според наши автори същността на този разузнавателен цикъл може да се раздели на две важни основни части, разделящи разузнаването на добиващо и аналитично. Добиващото разузнаване набавя разузнавателна информация на базата на поставени информационни задачи със средствата на оперативно-разузнавателна дейност, електронно разузнаване, разузнаване чрез открити източници, разузнаване чрез изображения и др. Аналитичното разузнаване от своя страна извършва информационно-аналитична дейност на основата на поставени информационни задачи, разработени на базата на постъпили заявки от различните потребители на разузнавателна информация, анализ на стратегическата среда за сигурност, дългосрочни тенденции за нейното развитие, произхождащи от това приоритети и съюзни ангажименти към разузнавателните общности, с които поддържаме сътрудничество и взаимодействие. Тези два компонента на разузнаването са взаимносвързани и зависими и не могат да бъдат реализирани и да функционират един без друг.

От гледна точка на своята функционалност разузнаването комплексно може да бъде разделено на разузнаване в интерес на националната сигурност и разузнаване, осигуряващо спазване на законодателството. Все по-често и интензивно, както и в перспектива, се разчита и на изкуствения интелект и неговата приложимост не само в интерес на разузнаването, а и като бъдещ домейн със стратегическо значение.

Първата фаза на информационния цикъл е определяне на изискванията към търсената информация: какво точно биха искали да знаят потребителите/заявителите и сроковете за изпълнение на поставените разузнавателни задачи. Важно е най-ценната информация да бъде отделена и съответното разузнаване да я докладва в определения срок. Щом информацията бъде добита, тя трябва да се свери/верифицира с наличната и да се вземе решение за нейната достоверност. Този процес на сравняване и записване на данните е автоматизиран и на него може да се разчита във висока степен. Въпреки това ролята на човешкия фактор остава основна по важност. Веднъж добита, съпоставена, разпределена по информационни масиви (архиви), разузнавателната информация следва да бъде обработена в кратка форма, като резюме, в което се акцентира на съществено. Тълкуването на информацията е дело на разузнавателните експерти, а разпространението ѝ е особено деликатна дейност, защото се случва предоставяне на висшето държавно ръководство на неточна, неблагоприятна или подвеждаща информация. Въпреки че не е честа практика, съществува възможност някои тълкувания на информацията да са изкривени или не съвсем точни, за да „паснат“ на нечии политически очаквания или предубеждения. По-лошо обаче е, когато доклади на разузнавателните служби изобщо се неглижират или не им се обърне достатъчно внимание. Но практиката е доклад, донесение, справка или друг информационен документ да носи точна, коректна, своевременна информация, подкрепена с доказателства, факти, коментари и преценки на съответните експерти.

От особена важност е и прогностичният характер на разузнавателната информация. Ефективността на разузнаването се основава на факта, че то е деполитизирано [2]. Неговото превръщане в бюрократична машина или част от административнобюрократичната държавна система е недопустимо. Спъването на регламентираната му дейност е пречка с много тежки последствия.

Разузнавателните служби допринасят съществено за намаляване на неопределеността и набелязване на алтернативни варианти на действие от вземащите решения чрез предоставената информация и аналитични продукти. За тази цел институциите от разузнавателната общност използват процедури и етапи с цикличен характер – това е т.нар. „разузнавателен процес“, чрез който те изпълняват разузнавателната си информационна мисия. Информационно-аналитичната дейност е специфичен познава-

телен процес, насочен към изследването на скрити и явни действия, процеси и явления, с потенциал за създаване на рискове или заплахи за сигурността на държавата, обществото, групи от обществото или отделни негови граждани [3].

Цялостният процес се състои от отделни процеси по събиране, обработване, систематизиране, съхраняване, анализиране, използване и предоставяне на информация на вътрешни и външни потребители. Информационната дейност включва мероприятия по предоставяне на аналитична информация на основата на отделни разузнавателни данни или обединяване и предоставяне на цялата налична информация, която е налична в информационния масив. Аналитичната дейност надгражда информационната, като на тази основа се анализират и извеждат съдържащите се в нея заплахи и рискове, потенциални неблагоприятни последици и се предлагат варианти на решения или превантивни мерки. На стратегическо ниво аналитичната дейност включва анализ на международната среда за сигурност, динамиката на процесите, обектите на заплахи и конкретните мерки за тяхното неутрализиране или ограничаване на въздействието и проявлението им. Прогностичната дейност отразява резултатите от дейността на аналитичните разузнавателни органи и от своя страна включва прогнозиране на посоката и очакваната степен на интензитет и изменение на рисковите фактори и заплахи. Разузнавателният цикъл включва още планиране и даване на указания; събиране на информацията; анализиране; обобщаване чрез изводи и хипотези; и изготвяне на крайни продукти – документите, които съдържат придобитото ново знание, на основата на което се предлагат варианти за взимане на решения. Предложените решения трябва да са кратки и ясни, аналитичната същност да е в началото (изводи), а след нея да последва т.нар. „градация на вероятности“ (решения).

Планирането и управлението на разузнавателния цикъл се реализира от държавното (политическото) ръководство и се състои от следните основни етапи: 1. идентифициране на приоритизиране на нуждите от разузнаване; 2. разработване на разузнавателна архитектура; 3. изготвяне на план за събиране на данни и факти; 4. издаване на съответни заповеди и заявки до разузнавателните структури за добиване на необходимата разузнавателна информация.

В рамките на НАТО координираното разузнавателно сътрудничество се реализира от CCIRM – The Collection Coordination Intelligence Requirements Management [5], съгласно Доктрината на Алианса за добив на разузнавателна информация. Процесът е сложен и гъвкав, изискващ бързо и ефективно прилагане на процесите на разузнавателния цикъл при вземане на решения.

По своята същност стратегическите решения са решения, взети в процеса на когнитивна управленска дейност, които са дългосрочни и всеобхватни, със значими и трайни последствия, свързани са с използването на големи и разнообразни ресурси и са скъпоструващи [4]. Те са в резултат на сериозни и задълбочени анализи и изследвания, с дълъг срок на действие, прогнози и предвиждания, както и с голям риск на сбъдване. Освен преките резултати от тези решения, които са дефинирани в техните цели, стратегическите решения пораждат и съществени косвени ефекти, които могат да бъдат от различно естество: трайни, дългосрочни, средносрочни или краткосрочни, общосистемни, нетрадиционни, окончателни или неокончателни, контекстуални и пр. Вземането им изисква потенциал да се мисли и разсъждава абстрактно за последствията във всички пространствени, времеви, ресурсни и др. аспекти, с оценка на причинно-следствените взаимозависимости в динамични и сложни системи със сложни отношения на действащите компоненти в тях.

Стратегическото решение е сложен, многоаспектен и дългосрочен процес на вземане на поредица свързани или отделни решения в условия на нелинейност, непос-

тоянство, неопределеност, неяснозначност, нееднородност и дефицит. Преките (първичните) ефекти от решенията са видими/налични след дълъг период от време, а непреките (вторичните) ефекти са налични, когато решението поражда допълнителна последователност от последствия [1]. В големите системи, каквато е Системата за защита на националната сигурност, първичните, вторичните и последващите ефекти са продукт на взаимовръзката и синергията в тяхната организация. Те са с общо въздействие и взаимно влияние. Силата на последващите ефекти заглъхва с увеличаването на техния порядък, но в теорията е описан и цикличнопулсиращ ефект, с дълги резониращи вълни и нелинеен спектър, чувствителен към начални допускания.

В общия случай не само косвените ефекти са трудни за предвиждане и проактивни действия, но е особено трудно да се разбере и причината на тяхната проява. Това изисква вземането (и подготовката) на стратегическото решение да е систематично и рационално, на базата на правилно разбиране на проблематиката, изводите и предложенията за нейното разрешаване. Тези решения е необходимо да бъдат подкрепени от всички, върху които имат ефект, с консенсус.

Стратегическите решения невинаги са ясни и еднозначни от пръв поглед. Това е така, защото са сложни и понякога трудни за цялостно разбиране и схващане на всички техни последици, сиреч многоаспектността и тяхната мултипредметност пречат за приемането им. Решенията ще са в сила за дълъг период от време, понякога над 20 или дори 50 години. С голяма доза на сигурност може да се прогнозира, че предпоставките и гледните точки, на които е базирано, ще се променят и повечето от зададените предположения при тяхната формулировка ще се изменят значително. Така вероятността решенията да не съответстват на бъдещите обстоятелства е твърде възможна, което пък сериозно да рефлектира върху основния техен замисъл.

Рискът от вземане на стратегически решения се дължи на това, че по принцип те изискват ангажираност на всички ресурси на системата. Възможно е решенията да се преразглеждат през определен период от време, когато обстоятелствата го изискват или обстановката се промени значително. Тогава тези решения подлежат на преформулиране и модифициране с цел осигуряване на устойчивост и цялост на развитието на системата. Допълнителна несигурност и риск внася фактът, че даже и преките последици понякога са трудни за определяне и остойностяване.

Разновидност на стратегическото решение е консенсусното решение. Неговото вземане е процес, който може да произведе значителни непреки ефекти от различно естество. Така е при по-малко рисковите решения. Освен това не всички решения, които са стратегически, са толкова дългосрочни, но дори и краткосрочните могат да бъдат разглеждани и съобразени в контекста на общите (дългосрочните) стратегически цели. Дори и не всички стратегически цели, даже и най-дългосрочните, са скъпи и свързани с използването на много ресурси. Но общо правило е, че консенсусното решение налага допускане на компромиси, наречени „стратегически компромиси“.

Стратегическите компромиси се случват за намиране на баланс между настоящи възможности и бъдещи очаквания. Стратегическото ръководство е изкуство да се направи удачен избор измежду конкуриращи се алтернативи, понякога и взаимноизключващи се. Компромисите измежду удовлетворителни дейности и/или поведение и желанието за максимализиране на резултатите за пределно кратко време предопределят сложността на оптималните стратегически решения в дългосрочен аспект.

Литература

1. **Алашки,** М. Вземане на решения в Системата за защита на националната сигурност. Монография. София: Принт фактор, 2022. ISBN 978-619-91280-3-9.

2. **Закон** за военното разузнаване. София: Апис. [онлайн]. [прегледан 7.07.2022]. *https://legislation.apis.bg/doc/2689930/0.*
3. **Иванов,** Е. Аналитично разузнаване. София: ВА „Г. С. Раковски“, 2021.
4. **Семерджиев,** Ц. Стратегия – среда, ресурси, способности, планиране. София: Класика и стил, 2007.
5. *http://acronymsandslang.com/definition.html.* [прегледан 26.07.2022].

COUNTERINTELLIGENCE AS A TOOL FOR PROTECTING THE STATE AND SOCIETY

Prof. Igor Britchenko, DES
Prof. Krzysztof Chochowski, DSc
State Higher Vocational School
Memorial of Prof. Stanislaw Tarnowski – Poland

КОНТРАРАЗУЗНАВАНЕТО КАТО ИНСТРУМЕНТ ЗА ЗАЩИТА НА ДЪРЖАВАТА И ОБЩЕСТВОТО

проф. д.и.н. Игор Бритченко
проф. д.н. Кшищоф Чоховски
Държавно висше професионално училище
„Мемориал на проф. Станислав Тарновски“ – Полша

Abstract: *The basic role of the state is to satisfy the primary human need, namely the need for security. To this end, it uses a number of instruments of a diverse nature, and counterintelligence is one of them. The scope of counterintelligence services has gradually expanded over time and currently includes not only counteracting hostile intelligence (sometimes also allied intelligence) but also combating organized crime (especially international), preventing the proliferation of weapons of mass destruction, combating terrorism (including cyberterrorism), controlling economic turnover in the field of dual-use technologies, combating individuals and groups seeking to overthrow the prevailing political order by force, combating extremism, cryptology, securing government communications, and finally protecting one's own intelligence operations. Counterintelligence is a kind of alter ego of intelligence, it is, as it were, the other side of the same coin. Adding the prefix kontr makes the basic word its opposite. Counterintelligence, unlike intelligence, which is supposed to obtain necessary information, protects it and ensures its safety. It is worth remembering, however, that counterintelligence is not only a defensive form of action, there is also offensive counterintelligence. Its aim, is to control the actions of the opponent, to manipulate them and influence them, to obtain information about the modus operandi the opponent, his contacts, interests, goals, state of knowledge. Therefore, counterintelligence should be referred to collecting information and taking actions to protect against espionage, other intelligence activities, sabotage or contract killings. Modern counterintelligence services face a number of new challenges, which are primarily related to the development of new ICT technologies, social media, and systems based on artificial intelligence, including machine espionage. They can be used to disrupt the electoral process, cause social unrest or even revolution (color revolutions), spread disinformation through fake news or using deep technology fake. Since modern societies are information societies, they are highly susceptible to information attacks aimed at persuading them to behave in a specific way, e.g. to vote for a specific candidate or protest against the policy of a given government. Modern information techniques allow for the manipulation of images and sounds, and thus enable the publication of false information, processed, manipulated to achieve a specific goal of information warfare. An example here is the deepfake technology, which, through ultra-realistic video materials, can change the perception of a given person in the public consciousness and influence the outcome of elections. Based on the above comments, it can be stated that today's counterintelligence, in addition to traditional challenges related to the protection and protection of its own systems and information resources, as well as an active form of counteracting espionage, must keep up with the development of new ICT technologies, social media, and systems based on artificial intelligence. Petrification in this area may lead to a decrease in its effectiveness, and consequently also to inefficiency and serious perturbations in the sphere of security.*

Key words: *counterintelligence; state security; purpose and tasks of counterintelligence; contemporary challenges for counterintelligence services*

Резюме: *Основната роля на държавата е да задоволява основната човешка потребност, а именно потребността от сигурност. За тази цел тя използва редица инструменти от*

различно естество и контраразузнаването е един от тях. Обхватът на контраразузнавателните служби постепенно се разширява с течение на времето и в момента включва не само противодействие на враждебното разузнаване (понякога и на съюзническото), но и борба с организираната престъпност (особено международната), предотвратяване на разпространението на оръжия за масово унищожение, борба с тероризма (включително кибертероризма), контрол на икономическия оборот в областта на технологиите с двойна употреба, борба с лица и групи, които се опитват да свалят със сила господстващия политически ред, борба с екстремизма, криптология, осигуряване на правителствените комуникации и накрая защита на собствените разузнавателни операции. Контраразузнаването е своеобразно алтер его на разузнаването, то е, така да се каже, другата страна на една и съща монета. Добавянето на префикса контра- превръща основната дума в нейната противоположност. Контраразузнаването, за разлика от разузнаването, което трябва да получи необходимата информация, я защитава и осигурява нейната безопасност. Струва си обаче да се помни, че контраразузнаването не е само отбранителна форма на действие – съществува и нападателно контраразузнаване. Неговата цел е да контролира действията на противника, да го манипулира и да му влияе, да получи информация за начина на действие на противника, неговите контакти, интереси, цели, състояние на знанието. Следователно контраразузнаването следва да се отнася до събирането на информация и предприемането на действия за защита от шпионаж, други разузнавателни дейности, саботаж или поръчкови убийства. Съвременните контраразузнавателни служби са изправени пред редица нови предизвикателства, които са свързани преди всичко с развитието на новите ИКТ технологии, социалните медии и системите, базирани на изкуствен интелект, включително машинния шпионаж. Те могат да бъдат използвани за нарушаване на изборния процес, предизвикване на социални вълнения или дори революции (цветни революции), разпространение на дезинформация чрез фалшиви новини или използване на дълбоки технологии за фалшифициране. Тъй като съвременните общества са информационни, те са силно податливи на информационни атаки, целящи да ги убедят да се държат по определен начин, напр. да гласуват за определен кандидат или да протестират срещу политиката на дадено правителство. Съвременните информационни техники позволяват манипулиране на изображения и звуци и по този начин дават възможност за публикуване на фалшива информация, обработена, манипулирана за постигане на конкретна цел на информационната война. Пример за това е технологията дийпфейк (дълбока фалшификация), която чрез свръхреалистични видеоматериали може да промени възприемането на дадена личност в общественото съзнание и да повлияе на резултата от изборите. Въз основа на горните коментари може да се заяви, че днешното контраразузнаване, освен традиционните предизвикателства, свързани със защитата и опазването на собствените системи и информационни ресурси, както и активната форма на противодействие на шпионажа, трябва да бъде в крак с развитието на новите ИКТ технологии, социалните медии и системите, базирани на изкуствен интелект. Петрификацията в тази област може да доведе до намаляване на нейната ефективност, а оттам и до неефективност и сериозни смущения в сферата на сигурността.

Ключови думи: *контраразузнаване; държавна сигурност; цел и задачи на контраразузнаването; съвременни предизвикателства пред контраразузнавателните служби*

Introduction

Every organization, including the most developed and complex, which is a state, takes action based on the data and information it has. The success of the activities it undertakes often depends on whether they are true and reliable. The fate of empires and states often depended on the proper reaction of the rulers to the information they received.

The secret services, which constitute a kind of nervous system of the state, its „eyes“ and „ears“, were and are extremely helpful in this respect. Their activities, on the one hand, focus on obtaining information of interest to decision-makers, and on the other, on protecting their own information resources. We can therefore say that while intelligence is a „sword“, counterintelligence is a „shield“ protecting against that „sword“.

The basic role of the state is to satisfy the primary human need, namely the need for security. To this end, it uses a number of instruments of a diverse nature, and counterintelligence is one of them. According to the Authors, the thesis that counterintelligence is in fact a tool for protecting the state and society from hostile acts aimed at the foundations of its existence and fundamental interests seems justified. The scope of counterintelligence services has gradually expanded over time and currently includes not only counteracting hostile intelligence (sometimes also allied intelligence) but also combating organized crime (especially international), preventing the proliferation of weapons of mass destruction, combating terrorism (including cyberterrorism), controlling economic turnover in the field of dual-use technologies, combating individuals and groups seeking to overthrow the prevailing political order by force, combating extremism, cryptology, securing government communications, and finally protecting one's own intelligence operations.

The purpose of this article is to highlight the role and importance of counterintelligence for the security of the state and its citizens. In addition, contemporary challenges facing counterintelligence will be identified.

The work uses the literary studies method as its leading method, with the historical and dogmatic methods used as auxiliary methods.

A research limitation is the inability to use classified information.

The entire discussion ends with conclusions, the implementation of which may contribute to increasing the efficiency and effectiveness of counterintelligence services.

The Origin of Counterintelligence

The origins of counterintelligence can be traced back to antiquity. Of course, counterintelligence at that time was not as structured and legally empowered as it is today. The scope of actions taken and tasks set was also much more modest, nevertheless counterintelligence was and played an important role in the context of state security. Interestingly, at that time state security was identified with the security of the ruler and his family. Therefore, counterintelligence activities focused primarily on eliminating conspiracies against the ruler's authority and preventing assassination attempts.

Already in ancient Hindu epic poems, i.e. *Mahabharata* and *Ramayana,* we can find fragments concerning both intelligence and counter-intelligence activities. For example, there is a statement that „A king should have confidence only in his own servants, although he should not fully trust them even. Treachery on the part of the king's advisors is the greatest defeat of a king" [52: 128]. The quintessence of counter-intelligence activities is formulated in this work in the following way: „A king should also spy on his advisors, friends and sons, his provinces, cities and areas that are under his authority. Having spies in shops, places of entertainment and gatherings, among beggars and wise men, in his own court and in the homes of his citizens, he should be able to recognize spies of the enemy" [52: 167].

In turn, *the Ramayana,* or *the Story of Rama,* indicates that „One should not hastily decide to use force against an opponent without attempts at reconciliation, bribery and sowing discord among enemies" [34: 185]. Naturally, a ruler, being aware of the threats, must have people and structures at his disposal that will counteract the aforementioned dangers, and therefore must have his own counterintelligence.

The issue of spying, intelligence and counterintelligence activities can be seen particularly clearly in Chinese writings of the ancient period, the leading representative of which is Sun Tzu – the author of the fundamental work of the period The *Art of War. The Art of War* is divided into thirteen chapters, two of which directly concern the issues of interest to us, i.e. intelligence and counterintelligence. These are Chapter I entitled *Reconnaissance* and Chapter XIII entitled *The Use of Spies.* We can find statements there that are

still relevant today. For example, Chapter I states that *„The strategy of war is cunning and creating illusions. Therefore, if you are capable of something, pretend to be clumsy; if you are active, create the appearance of passivity. If you are close, create the appearance of a great distance; if they believe you are far away, find yourself unexpectedly close. Try to mislead the enemy, create disorganization in his army and only then strike"* [47: 11]. In Chapter XIII, summing up his considerations on intelligence and counterintelligence, Sun Tzu stated that *„An army without secret agents is truly like a blind or deaf man"* [47: 83].

Chinese thought radiated to medieval Korea and Japan, which creatively adapted Sun Tzu's views, developing them and adapting them to local political and social realities. In the latter, extensive fragments of Sun Tzu's *Art of War were translated* in his work *Shoku Nihongi* from 747, which is considered the official history of Japan. Deception, betrayal, assassination, gathering information about the enemy, his disinformation were the everyday life of the time, in which counterintelligence played an important role.

We can also find counterintelligence services among the Assyrians, Babylonians, and Persians [40: 3]. Political murders and assassinations of rulers forced them to take more care of their security. One of them, namely Zimri The Lim ruler of the Mari kingdom, who ruled from 1775 to 1761 BC, was advised never to move alone and to use agents to test the loyalty of his servants and officials [43: 11].

Also in the Bible, in the Old Testament, we can find passages that prove that the Israelites and the peoples and tribes of their time understood the importance of intelligence and counterintelligence. Failures in this area often ended in the destruction and annihilation of the entire population. For example, the capture of the strategic city of Jericho by Joshua's troops was possible, among other things, thanks to the infiltration of its fortifications by two spies. They got inside and carried out their mission using the help of a local prostitute named Rahab. The chosen people achieved a decisive victory here, which enabled the further conquest of the Promised Land. The defeat, on the other hand, was the loss of a kind of Wunderwaffe in the form of Samson, from whom Delilah, an agent of the Philistines, had cunningly obtained information about the source of his strength . She used this knowledge by cutting his hair, thereby depriving Samson of his supernatural strength. As can be seen, in this case what we would today call counterintelligence cover failed, as Samson was allowed access and he succumbed to the „swallow" or „sweet bait" [44: 19 et seq.; 19: 517 et seq.; 23: 110 et seq.].

Over time, agent activity began to take on an increasingly organized and formalized framework. The strengthening of the state's executive apparatus, the abandonment of perceiving the state as the property of the ruler and the people living in it as subjects in favor of citizens, the development of diplomacy, the industrial revolution, the emergence of new technologies, all this meant that in principle in every country special services were established (including counterintelligence services – K. Ch.). Their style of operation depends on the political regime prevailing in a given country and its internal and external situation, as well as the applicable law [11: 42].

It can therefore be stated that the genesis of modern intelligence and counterintelligence agencies dates back to ancient times and is essentially connected with the state powers of the time [17; 6; 43; 37; 35; 49; 42; 5; 20; 40; 41; 39; 15; 38; 4; 18; 3; 19; 44; 11; 23]. Of course, one cannot put an equal sign between the services of the ancient era and the modern ones, nevertheless the basic purpose and scope of their activities have not changed, constituting a common, timeless denominator.

The essence and purpose of counterintelligence

Counterintelligence is a kind of *alter ego* of intelligence, it is, as it were, the other side of the same coin. Adding the prefix kontr- makes the basic word its opposite. Counterintelligence, unlike intelligence, which is supposed to obtain necessary information, protects

it and ensures its safety. It is worth remembering, however, that counterintelligence is not only a defensive form of action, there is also offensive counterintelligence. Its aim, as B. Piasecki points out, is to control the actions of the opponent, to manipulate them and influence them, to obtain information about *the modus operandi* the opponent, his contacts, interests, goals, state of knowledge [33: 262]. Therefore, according to A. Kowalski, counterintelligence should be referred to collecting information and taking actions to protect against espionage, other intelligence activities, sabotage or contract killings [25: 278].

Counterintelligence can be understood in at least two ways, namely functional and institutional. The first is related to the tasks that counterintelligence performs and the information that it obtains through its activities. The second way, institutional, is that counterintelligence is perceived as an institution, an organization operating, in principle, within the geographical borders of a state [32: 26, 27].

According to M. Minkina, the term *counterintelligence should be* understood as combating all hostile intelligence activities and other hostile activities of foreign entities, against which the state should be protected using passive and active methods. Passive methods include measures that prevent access to the state's information resources. Active measures, on the other hand, include those activities that involve identifying the activities of foreign intelligence services, their objects of interest, and the methods used [28: 367, ff].

Counterintelligence is defined within NATO as activities related to identifying and countering threats to security from hostile intelligence agencies and organizations or individuals engaged in espionage, sabotage, diversion or terrorism [16: 118]. From the previously cited NATO definition of counterintelligence, it follows that we can distinguish four basic types of counterintelligence activities, i.e.: countering espionage, combating sabotage, diversion or terrorism [23: 93].

Counterintelligence activity is an activity aimed at neutralizing or acquiring foreign intelligence services for one's own intelligence activities, as well as the penetration of foreign intelligence by a „mole“, as well as activities aimed at protection against espionage, sabotage and other activities foreign intelligence [2: 305]. This activity is aimed at disrupting or, best of all, breaking the intelligence cycle of a foreign state, the subject of which is the state implementing broadly understood counterintelligence cover. In turn, according to L. K. Johnson, it is the thwarting of hostile operations directed against one's own secret services and the state, by foreign secret services or terrorist organizations [22]. Its ultimate goal is to take control of the operations of the enemy's secret services and manipulate their actions to one's own advantage [48: XXI]. On the other hand, LE Sullivan, is of the opinion that counterintelligence activities include investigations into cases involving espionage, terrorism, sabotage of technology, computer infiltration and other specialized counterintelligence operations [45: 858].

A similar view is presented by P. J. Redmond, who points out that in the USA it is assumed that counterintelligence activities consist in gathering information and taking actions to identify, deceive, use, disrupt or protect against espionage, other intelligence activities, sabotage or assassination carried out on behalf of foreign powers or their representatives, as well as international terrorist organizations. He then adds that these are special activities of security organizations (special services – K. Ch.), which are authorized and managed by the government in order to protect the state and its citizens from espionage, sabotage and terrorism [36]. In turn, in the USSR and then Russia, counterintelligence activities are activities undertaken by special services, on the basis of special authorizations, consisting in combating the intelligence services of other countries and the subversive activities of organizations and individuals used by these services. In the Russian cultural circle, counterintelligence is considered one of the instruments of political power of states. In the United King-

dom, counterintelligence activities protect national security against threats posed by espionage, terrorism and sabotage, and against actions aimed at overthrowing or destroying parliamentary democracy [44: 239, ff].

For this reason, in the case of counterintelligence activities, four leading areas can be distinguished, namely: intelligence organizations of foreign countries; extreme illegal (extremist) organizations operating in their own country; foreign and domestic terrorist organizations; and economic activities that threaten the security or functioning of the state [51: 15].

Counterintelligence activities are therefore aimed at detecting and preventing internal and external threats to the state [21; 14]. As M. Minkina points out, counterintelligence is to prevent foreign intelligence services or foreign movements and groups, often inspired and supported by intelligence services, from accessing information constituting a state secret [28: 45].

As V. Mitrokhin emphasizes, counterintelligence activities can be used to take steps in advance to prevent hostile actions aimed at the security of the state [30]. An important role in this process is played by deception of opponents, which is a proactive and anticipatory action against the opponent.

Based on the above remarks, it should be stated that the essence of counterintelligence today goes far beyond its original understanding and boundaries. Today, it is not only counteracting espionage and protecting one's own information resources, but also covering one's own intelligence operations and deception of the enemy. Counterintelligence cannot therefore be understood as a passive element of the state's security system, which only reacts to the enemy's actions. On the contrary, it should be active and full of initiative in order to impose its will on the other side and achieve victory.

The purpose of counterintelligence, as stated by M. Minkina, is to detect the activities of foreign intelligence services, to prevent them from functioning, and to destroy or neutralize the results of the work of foreign intelligence. Counterintelligence therefore includes combating all hostile intelligence activities and other hostile activities of foreign entities, from which the state must be protected, using passive and active methods [28: 367]. J. R. Clark approaches this issue similarly, according to whom, protecting our intelligence operations and other secrets from those who want to learn them or betray them, is precisely the purpose of counterintelligence [13: 1; 26: 319].

The purpose of counterintelligence is also to influence the decisions of the opponent as a result of one's own disinformation and deception activities . Misleading the enemy, deceiving him, or even better, making him accept the vision of reality we desire – these are the manifestations of the so-called active counterintelligence. Its goals, as B. Piasecki points out, are: identifying and understanding the opponent; penetrating his structures; effectively neutralizing his actions; using them for one's own purpose [32: 269]. In addition to offensive counterintelligence, there is defensive counterintelligence, the goal of which is to passively protect one's own information resources and conducted operations. As a result, the broadly understood public security will appear as the fundamental goal of counterintelligence.[1]

Challenges for modern counterintelligence services

Modern counterintelligence services face a number of new challenges, which are primarily related to the development of new ICT technologies, social media, and systems based on artificial intelligence, including machine espionage. They can be used to disrupt the electoral process, cause social unrest or even revolution (color revolutions), spread disinformation through fake news or using deep technology. fake . However, we must not lose

[1] Public security is understood as a state where the general public of a given country is free from dangers, regardless of their source, and the existing legal order is protected against violations (For more information, see e.g.: [12: 265-279]).

sight of acts of sabotage, the outbreak of which we are seeing in connection with the war in Ukraine. A number of fires in Poland and other EU and NATO countries were started by sabotage groups financed by the Kremlin and carrying out Moscow's orders.

Since modern societies are information societies, they are highly susceptible to information attacks aimed at persuading them to behave in a specific way, e.g. to vote for a specific candidate or protest against the policy of a given government [1: 13]. Modern information techniques allow for the manipulation of images and sounds, and thus enable the publication of false information, processed, manipulated to achieve a specific goal of information warfare [50: 173]. An example here is the deepfake technology, which, through ultra-realistic video materials, can change the perception of a given person in the public consciousness and influence the outcome of elections [10: 61-78].

„The advancement of deepfake technology increases the risk of spreading false information, which directly undermines the credibility of news, information, and interpersonal exchanges" [24: 158, 159]. Using deepfake technology fake it is possible to sabotage both people and institutions. You can present anything that is humiliating, e.g. bribery, adultery, etc. [46: 1015]. Counterintelligence can successfully play the role of unmasking and exposing lies, as can be seen in the example of the current presidential elections in Romania.

It is also worth mentioning the challenges related to the emergence and development of disinformation systems, including those based on AI. For special services, various shades of disinformation in the form of lies, deceit, fraud, manipulation – are something natural [27: 792; 29; 8: 223 – 231]. Harnessing AI to these activities and processes multiplies and intensifies their effectiveness. The same applies to machine espionage, which significantly affects the intelligence cycle. It can be used to help analysts overcome the „data smog" and find the proverbial needle in a haystack [31: 6]. As a result, it becomes possible to establish connections between individuals and detect, for example, agents of enemy intelligence, carry out information operations using deepfake technology, or finally determine money transfers and identify both their addressees and recipients [9: 5]. Machine espionage enables the quick identification of disinformation systems based on new technologies, including those based on artificial intelligence. Fake news, deep fake, „resonance boxes", as well as enemy agents, can be identified and eliminated much more efficiently, thanks to artificial intelligence and tools based on them [7: 229].

Based on the above comments, it can be stated that today's counterintelligence, in addition to traditional challenges related to the protection and protection of its own systems and information resources, as well as an active form of counteracting espionage, must keep up with the development of new ICT technologies, social media, and systems based on artificial intelligence. Petrification in this area may lead to a decrease in its effectiveness, and consequently also to inefficiency and serious perturbations in the sphere of security.

Conclusions

1. The basic role of the state and its administrative apparatus is to ensure security for entities subject to its authority. An important role in this process is played by secret services, including, of course, those we call counterintelligence.
2. The origins of counterintelligence can be traced back to antiquity. Over time, their role and the scope of their activities have expanded.
3. Counterintelligence is a kind of *alter ego* of intelligence, it is, as it were, the other side of the same coin. Counterintelligence protects information and ensures its security.
4. The purpose of counterintelligence is to detect the activities of foreign intelligence services, to prevent them from functioning, and to destroy or neutralize the results of the work of foreign intelligence. Counterintelligence uses passive and active methods.

5. Counterintelligence is a fundamental tool for protecting the state and society.

6. The effectiveness of counterintelligence as a tool above is determined by its ability to adapt and incorporate new ICT technologies into its operations. However, this does not mean disregarding the personal sources of counterintelligence.

Bibliography

1. **Aleksandrowicz,** T. R. Mechanizmy ataku informacyjnego. Skuteczność przeciwdziałania. – W: *Dezinformacja* – Inspiracja – Społeczeństwo. Social CyberSecurity. Pod red. D. Boćkowskiego, E. Dąbrowskiej-Prokopowskiej, P. Goryń, K. Gorynia. Białystok, 2022.
2. **Allen,** T. B., N. Polmar. Księga szpiegów. Encyklopedia. Warszawa, 2000.
3. **Andrew,** Ch. The secret world. A History of Intelligence. London, 2018.
4. **Brzeski,** R. Wojna informacyjna – wojna nowej generacji. Komorów, 2014.
5. **Campbell,** B. Greek and Roman Military Writers: Selected Readings. Routledge, 2004.
6. **Cardwell,** J. M. A Bible Lesson on Spying. – In: *Studies* in Inteligence, 1978, t. 22, nr 3.
7. **Chochowski,** K. Szpiegostwo maszynowe szansą i wyzwaniem dla służb specjalnych. – W: *Zagrożenia* i wyzwania bezpieczeństwa w cyberprzestrzeni. Pod red. M. Pomykała, I. Oleksiewicz. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów, 2024.
8. **Chochowski,** K. Dezinformacja w administracji publicznej. – W: *Założenia* nauki administracji. Pod red. J. Smarż, S. Fundowicz, P. Świtał. Wyd. Wolters Kluwer. Warszawa, 2024.
9. **Chochowski,** K. Basic determinants of special services efficiency. – W: *Košická* Bezpečnostná Revue, Vol. 13, No. 1, 2023.
10. **Chochowski,** K. Wykorzystanie technologii deepfake w operacjach informacyjnych w aspekcie historycznym i współczesnym. – In: *International* Journal of Legal Studies, 2023, Vol. 13, No 1.
11. **Chochowski,** K. Służby specjalne w Polsce. Sofia, 2021.
12. **Chochowski,** K. Bezpieczeństwo publiczne jako dobro publiczne. – W: *Dobra* publiczne w administracji. Pod red. M. Woźniak, E. Pierzchała. Toruń, 2014.
13. **Clark,** J. R. Intelligence and National Security: A Reference Handbook. London, 2007.
14. **Coletta,** G. Defining Counterintelligence. CI, Security and non-governmental actors. GRIN Verlag, 2017.
15. **Crowdy,** T. Historia szpiegostwa i agentury. Warszawa, 2010.
16. **Dictionary** of terms and definitions NATO AAP – 6, p. 118. [online]. *http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf.*
17. **Dvornik,** F. The Origins of Intelligence Services. New Brunswick, NJ: Rutgers University Press, 1974.
18. **Encyclopedia** of Intelligence and Counterintelligence. Vol 1-2. Edited by: R. P. Carlisle. Routledge, 2015.
19. **Formicki,** T. Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej. Warszawa, 2020.
20. **Herzog,** Ch., M. Gichon. Battles of the Bible: A Military History of Ancient Israel. Greenhill, 2005.
21. **Ibp,** U. Ukraine Intelligence & Security Activities and Operations Handbook. Washington, 2006.
22. **Johnson,** L. K. National Security Intelligence. – W: *The* Oxford Handbook of National Security Intelligence. Edited by L. K. Johnson. Oxford, New York, 2010.
23. **Kamiński,** M. A. Ewolucja wywiadu jako instytucji państwa. Warszawa, 2021.
24. **Kaur,** A., A. N. Hoshyar, V. Saikrishna, S. Firmin, Feng Xia. Deepfake video detection: challenges and opportunities. – In: *Artifcial* Intelligence Review, 2024, Vol. 57, No. 159.
25. **Kowalski,** A. Kontra. Sztuka walki z wywiadem przeciwnika. Łomianki, 2022.
26. **Larecki,** J. Wielki leksykon służb specjalnych świata. Warszawa, 2007.
27. **Miller,** S. National security intelligence activity: a philosophical analysis. – In: *Intelligence* and National Security, 2022, Vol. 37, No. 6.
28. **Minkina,** M. Sztuka wywiadu w państwie współczesnym. Warszawa, 2022.
29. **Minkina,** M., B. Gałek. Kłamstwo i podstęp we współczesnym świecie. Warszawa, 2015.
30. **Mitrokhin,** V. KGB Lexicon: The Soviet Intelligence Officers Handbook. London, 2002.
31. **Moran,** Ch. R., J. Burton, G. Christou. The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. – In: *Journal* of Global Security Studies, 8(2), 2023.
32. **Piasecki,** B. Kontrwywiad. Atak i obrona. Łomianki, 2021.

33. **Piasecki,** B. Kontrwywiad ofensywny jako element systemu bezpieczeństwa państwa. – W: *Przegląd* Bezpieczeństwa Wewnętrznego, nr 10/2014.
34. **Ramajana.** Adaptacja E. Walter. Warszawa, 1993.
35. **Rankov,** N. B. Exploratio. Military and Political Intelligence in the Roman World from the Second Punic War to the Battle of Adrianople. London: Routledge, 1998.
36. **Redmond,** P. J. The Challenges of Counterintelligence. – In: *The* Oxford Handbook of National Security Intelligence. Edited by L. K. Johnson. Oxford, New York, 2010.
37. **Richmond,** J. A. Spies in Ancient Greece. – In: *Greece* & Rome, 1998, Vol. 45, No 1, Cambridge University Press.
38. **Sheldon,** R. M. A Guide to Intelligence from Antiquity to Rome. – In: *The* Intelligencer, Vol. 18, No. 3, 2011.
39. **Sheldon,** R. M. Szpiedzy, wywiady i tajne służby. Warszawa, 2008.
40. **Sheldon,** R. M. Intelligence Activities in Ancient Rome: Trust in the Gods But Verify. Routledge, 2007.
41. **Sheldon,** R. M. Spies of the Bible. Greenhill Books, 2007.
42. **Sheldon,** R. M. Espionage in the Ancient World. McFarland & Company, 2003.
43. **Sheldon,** R. M. Spying in Mesopotamia: The World's Oldest Classified Documents. – In: *Intelligence,* Vol. 33, No. 1, 1989.
44. **Słoń,** M., S. Wójcik. Tajemnice wywiadu wewnętrznego. Warszawa, 2020.
45. **Sullivan,** L. E. Encyclopedia of Law Enforcement. Vol. 1. London, 2005.
46. **Temir,** E. Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism. – In: *Selçuk* İletişim Dergisi, 2020, Nr. 13 (2).
47. **Tzu,** Sun. The Art of War. [online]. *https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=0ahUKEwiX1v7PmuLRAhWEvhQKHbalCxYQFggggMAA&url=http%3A%2F%2Fwww.lazarski.pl%2Fpl%2Fdownload%2F837%2F&usg=AFQjCNH1t9EbkxgRycY2z_Fc8ct9L_xRA&sig2=saTmVXw7cKwS4AkHAmn8Rg&bvm=bv.145393125,bs.2,d.bGg&cad=rja.*
48. **West,** N. Historical Dictionary of Cold War Counterintelligence. Plymouth, 2007.
49. **Whitehead,** D. Aineias the Tactician. How to Survive Under Siege. Bristol Classical Press, 2002.
50. **Wrzosek,** M. Wojny przyszłości. Doktryna, technika, operacje militarne. Warszawa, 2018.
51. **Zalewski,** S. Służby specjalne w państwie demokratycznym. Warszawa, 2002.
52. *http://tlvp.net/~b.mikolajewska/booknook/Mahabharata/PDF/Slimmed.n.Trimmed/MahabharataKs12a.pdf*

ДОБИВАНЕ НА ОПЕРАТИВНА ИНФОРМАЦИЯ ЧРЕЗ ВЪЗДУШНИ СРЕДСТВА В КРИЗИСЕН РАЙОН И ПРЕДАВАНЕТО Ѝ В РЕАЛНО ВРЕМЕ В УПРАВЛЯВАЩИЯ ОРГАН

проф. д-р Евгени Манев
Университет по библиотекознание и информационни технологии – София

OBTAINING OPERATIONAL INFORMATION VIA AERIAL MEANS IN A CRISIS AREA AND TRANSMITTING IT IN REAL TIME TO THE MANAGING AUTHORITY

Prof. Evgeni Manev, PhD
University of Library Studies and Information Technologies – Sofia

Резюме: *Изготвянето на концепции и стратегии за информационно осигуряване в кризисни ситуации с цел адекватно и компетентно управление на силите и средствата е от ключово значение за възможно най-ефективно справяне с тях и намаляване до възможния минимум на негативните последствия за държавата и гражданите. В анализите е приложен мултидисциплинарен подход чрез интерпретация на теоретични знания за системите, общото учение за държавата, общото учение за сигурността, теорията за организационно-културния модел на организацията. На концептуално и стратегическо ниво е синтезиран модел за добиване на оперативна информация чрез въздушни средства в кризисен район и предаването ѝ в реално време в управляващия орган на държавата.*

Ключови думи: *информация (оперативна, в реално време); сигурност; криза; система*

Abstract: *Preparation of concepts and strategies for information provision in crisis situations, with the aim of adequate and competent management of forces and resources, is of key importance for the most effective possible handling of them and reducing to the minimum possible the negative consequences for the state and citizens. The analyses have applied a multidisciplinary approach through the interpretation of theoretical knowledge about systems, the general teaching of the state, the general teaching of security, the theory of the organizational-cultural model of the organization. At the conceptual and strategic level, a model has been synthesized for obtaining operational information by air means in a crisis area and its transmission in real time to the governing body of the state.*

Key words: *information (operational, real-time); security; crisis; system*

Увод

Придобиването на вярна, своевременна, точна, конкретна и пълна информация за състоянието на силите, средствата, физико-географските, природните условия, концепциите, стратегиите и плановете за действие на външни агенти (държава или държави, или други неприятелски настроени структури), имащи интерес от предизвикване на криза, за нагласите на населението и различните социални групи – политически, икономически и др., в кризисния район, както и други елементи, представляващи интерес за нас, е от решаващо значение за изготвянето на адекватни концепции, стратегии и планове за действие на оторизираните държавни органи, икономиката на държавата и населението с цел намаляване на рисковете и избягване на заплахите за интересите на държавата, хората, стопанските и други инфраструктурни обекти. Тези рискове и заплахи могат да бъдат в мирно време за нанасяне на щети или заплахи за

материални средства и ресурси, производствена или друга инфраструктура, разпространение на епидемии, пандемии или да са свързани с информация за терористични дейности или въоръжено нападение на страната и др.

Изложение

Придобиването на възможно най-пълна информация за процесите и състоянието на кризисния район изисква системен подход. Това означава, че всички ресурси на държавата за придобиване на информация трябва да са организирани като единна цялостна система, което означава да работят като една организация – т.е. под едно общо ръководство, обща от гледна точка на постигане на държавата цел, да са изградени на основата на единна обща концепция и стратегия. В този подход ключовото понятие е *„система“*, поради което се позоваваме на общата теория на системния подход. В научната общност е добре известно, че един от основоположниците на системния подход е английският естествоизпитател и изследовател на социалните явления Г. Спенсър, според когото „светът е едно цяло, имащо съставни части, които функционират съвместно. Това цяло е по-голямо от сбора на неговите части и определя тяхната природа (същност). Компонентите (частите) се намират в непрекъснато взаимодействие и не могат да бъдат извън системата (цялото). В тази теория се използват два общи подхода на изследване – епистемологичен (от абстрактното към конкретното) и емпиричен (от конкретното към общото), прилагат се основните системни парадигми, подходи и методи на изследване на различни природни, техногенни, биологични и социални системи“ [2: 32].

От посочения системен подход следва изводът, че цялостното и пълно осигуряване на изпълнителната власт в държавата за целите на нейното адекватно на ситуацията управление (оценка на обстановката, вземане на решение и реакция) в условията на кризи следва да се изгражда, планира, организира и провежда (на концептуално ниво и на практика) като *специална рекурсивна (социална) кризисна система*. В състава ѝ следва да се приложи концепцията за организационно строителство и функциониране на *специална рекурсивна информационна система*. А в състава на тази информационна система следва да се изградят (някои от тях функционират в държавата) рекурсивни системи за различните видове информационно осигуряване, които могат да се обобщят като разузнавателни и контраразузнавателни. В състава на *рекурсивната разузнавателна система* следва да са организационно вградени всички системни елементи на държавата, осигуряващи разузнавателна информация. В този състав следва да бъде включена и *системата за придобиване на информация чрез използване на въздушни средства* и техните технологии за тази цел. В доклада не се разглеждат въпросите за използването на космическите средства и технологии за информационно осигуряване, които също трябва да са включени в националната държавна разузнавателна система.

Такъв системен подход изисква реализиране на концепцията за създаване на единен ръководен оперативен (ситуационен) информационен център в държавата, в който да се събира, обработва, съхранява, разпределя до ползвателите необходимата им информация; да се генерира и управлява знанието, свързано с управлението на силите (личния състав) и средствата за превенция и реакция при кризи. Само така може да се реализира концепцията за прилагане на системния подход, което от теоретична и практическа гледна точка е научнообоснован концептуален модел за подобряване на резултатите от работата на всички досега съществуващи специални организационни структури в тази област. Липсва цялостно завършена по форма и съдържание системна организация на силите и средствата за справяне при кризи в държавата. Това

не означава непременно разкриване на нови щатове в държавните и частните организационни структури, имащи отношение към управлението на силите и средствата за планиране, превенция и по-ефективно преодоляване на кризисни ситуации.

След като на концептуално ниво е определено мястото на *рекурсивната система за придобиване на оперативна информация чрез въздушни средства,* анализите в доклада се съсредоточава върху нея. Всички други въпроси, свързани с останалите елементи на специалната рекурсивна държавна информационна система, ще се споменават, но няма да се анализират поради невъзможността това да се извърши в един доклад – резултат на индивидуално авторско усилие. Така поставената цел на доклада изисква дефиниране на някои основни понятия, които се използват по-нататък.

Ключовото понятие *„информация“* е свързано с понятията „сигнал“, „данни“, „информация“, „знание“. Сигналът е физически носител, който отразява някакво състояние или неговата промяна. Когато на сигнала се даде конкретно значение (символиране по Лесли Уаит) [8], напр. промяна на електрическо напрежение, атмосферно налягане, температура на околната среда и др., на ниво на високите води на река, язовир и др., той, сигналът, става данна за това, за което е предназначен. При обработката на различни данни, касаещи някакъв процес, се генерира информация за него. Анализите на различните информации от процеса генерират знание за него. След генериране на знание от различните разузнавателни и контраразузнавателни системи важен става въпросът за управление на знанието в *специална рекурсивна информационна система.*

Понятието *„криза“* се интерпретира по различен начин в научната литература и в практиката, в зависимост от това в коя сфера на човешката дейност е нейното проявление, напр. социалната, екологичната, природната, техногенната, военната и др. Поради това е важно как се дефинират същността и съдържанието на понятието *„криза“* на концептуално ниво. В литературата има много изследвания на същността и съдържанието на кризите, наличие на много определения на това понятие. Според Л. Милушев тя е „Крайно изостряне на разрушителни процеси в дейността на лидера или организацията, предизвикано от скрита или явна стагнация (деградация) или поради бърз растеж (прогрес), който може да засегне на практика всяка съставна от функциите на институцията или индивида“ [7: 14 – 18].

Според Р. Маринов „*кризата* е сложна ситуация (или последователност от трудни ситуации), възел от проблеми, които застрашават базовите интереси на институцията, като поставят под въпрос самото ѝ съществуване“ [6: 40 – 45].

Според С. Денчев и др. *„кризата“* е промяна на регионалната, националната или международната обстановка, характеризираща се с увеличена интензивност на разрушителни или агресивни процеси. Тя е внезапна или промяна на установения начин на живот, предизвикана от човешка дейност, събития или природни явления. (...) Действието ѝ се предшества от обективни фактори“ [1: 33].

Ако се позовем на мултидисциплинарната интерпретация на общата теория на системите, организационните теории на организационно-културния модел на организацията, на концептуално ниво може да се дефинира, че: „*Сигурността* е динамично състояние, при което организацията функционира и работи съгласно плановия алгоритъм и правила в рамките на допуските на стойностите на нейните, на външната и на вътрешната среда параметри, и ако по някакви причини излезе извън рамките на плановото функциониране и работа, тя има ресурси (сили и средства) да го възстанови“ [3: 262 – 274].

Имайки предвид общото семантично съдържание на посочените по-горе определения на понятието *„криза“* и неразривната ѝ връзка с понятието *„сигурност“,* както и на посочения методологически мултидисциплинарен подход за изработване

на определение на понятието *„сигурност“*, на концептуално ниво може да се определи, че *кризата* е динамично състояние на *системата* (социална или друга), при което тя е изведена (или се извежда) от режима на нормалното ѝ функциониране, независимо какви са причините за това, и се намира в авариен или катастрофален режим на функциониране [4: 7 – 13]. За възстановяване на нормалното функциониране *системата* трябва да разполага с предварително подготвени сили и средства, които да използва за възстановяване на нормалното си функциониране. В противен случай нейната дълбока системна реорганизация или разпад са неизбежни.

От анализа на посочените дотук основни понятия следва изводът, че успешното справяне с кризи зависи от две критични рекурсивни организационни системи, които са системни елементи на рекурсивната социална система държава, – *специалната рекурсивна информационна система* и *специалната рекурсивна система за реакция/справяне при кризи*.

Понятието *„оперативна информация“* в доклада се разглежда в контекста на придобилата гражданственост англосаксонска концепция – като информация за ежедневно управление на ниво мениджъри и ръководители на екипи. Следва да се отбележи, че понятието „оперативно ниво на управление“ е елемент, свързващ стратегическото и тактическото ниво на организационното управление. Следователно в контекста на темата на доклада под *„оперативно управление“* е прието да се разбира текуща информация в реално време, необходима за управление на текущите ответни (реактивни) дейности по време на кризи. Следователно оперативна е тази информация, която е свързана с целите на оценка на текущата обстановка, вземане на решение и неговото изпълнение в хода на зараждане и развитие на кризисна ситуация.

Понятието *„информация в реално време“* означава същата да пристига в оторизираните управляващи и изпълнителски организационни структури с минимално възможното закъснение, което да осигури време за възможно най-бързо вземане на управленски решения и привеждане в действие на оперативните сили за възможно най-бърза ответна реакция в района на кризата. Това означава в момента на появяване на информация за даден процес в кризисния район да се приложи адекватна ответна реакция. Тази концепция изисква в държавата да се изгражда и усъвършенства на концептуално и стратегическо ниво *рекурсивната система за защита при кризи.* Това означава, че при този концептуален подход организационната стратегия за повишаване на ефективността на информационното осигуряване в нормални и кризисни условия, както и възможностите за максимално бърза превантивна и тактическа реакция трябва да има предварително подготвени сили и средства на държавата (и сега има такива), които напълно да отговарят на системните теоретични знания по организационна форма и съдържание на изискванията за рекурсивна *специална система за превенция и действия при кризи*.

Логически следва да се дефинират: *концепция*, *цел, мисия, визия, стратегия, функции, задачи* и *организационна структура на рекурсивната система за придобиване на оперативна информация чрез въздушни средства,* която за краткост ще наричаме *„въздушна информационна система“ (ВИС).*

Концепцията за изграждане на съвременна ВИС на държавата е, че чрез създаване на теоретичен модел на ВИС и неговото апробиране, валидиране и верифициране да се докажат и подобрят (при необходимост) оперативните способности, след което да се обединят съществуващите към момента способности в различните авиационни организационни структури в държавата, които да се развият до необходимите. Всичко това да се реализира в доказано разумен кратък срок.

Целта на ВИС е да придобива своевременна точна вярна и пълна информация чрез въздушни средства и технологии, необходима за целите на *специалната рекурсивна информационна система,* която е елемент от *специалната рекурсивна кризисна система* на държавата.

Мисията на ВИС е да осигурява специфична разузнавателна и контраразузнавателна информация и да генерира знания чрез използване на специфични въздушни средства и технологии, оперирайки в домейна *въздушно пространство,* за която другите специални информационни системи в държавата нямат такива оперативни способности. По този начин се допълва информационната картина за кризисния район с информация в реално време.

Визията за изграждане на ВИС в държавата е чрез изграждане на нормативно регулирани системни връзки да се създаде система на основата на съществуващите въздушни средства и техните разузнавателни, контраразузнавателни и специални оперативни способности към момента, които са в различни държавни и частни организации, които да функционират като едно цяло. Това в никакъв случай не означава тяхното организационно обединяване в една нова организация и извеждането им от състава на сегашните организации.

Стратегията за реализиране на ВИС може да включва следните основни етапи:

1. изготвяне, приемане и утвърждаване на държавно ниво на теоретичния модел на системата;
2. включване в системата на съществуващите в държавата оперативни способности според утвърдения модел;
3. стартиране на работата на системата;
4. развитие на нови оперативни способности съгласно теоретичния модел;
5. периодични анализи и усъвършенстване на модела.

Основни функции на ВИС

Базови принципи, на които следва да се изграждат основните функции:

1. Въздушните средства – собственост на държавни, частни или публичночастни организации, изпълняват функциите и задачите си във ВИС съгласно нормативно уредените им правомощия, без да се извеждат от организационните структури, които ги притежават, изпълнявайки предназначението си в тях.

2. Въздушните средства, изпълняващи разузнавателни/контраразузнавателни и специални функции, принадлежащи на държавни, публичнодържавни и/или частни организации, планират, организират и осъществяват функциите и задачите си, като предоставят придобитата информация на управляващия орган на ВИС. Регулирането на тези взаимоотношения се уреждат нормативно в държавата.

3. Изграждането на разузнавателен, контраразузнавателен или специален капацитет [5: 164 – 172] в операторите на въздушни средства в интерес на информационното осигуряване на ВИС се осъществява с държавно, публичночастно или частно участие (финансиране и др. способи) под контрола на държавата (уведомителен, разрешителен, лицензионен и др. режим).

4. Изпълнението на разузнавателни, контраразузнавателни или специални задачи в интерес на превенцията и справянето с кризи се извършва планово и по заявка на държавата чрез ВИС, която осигурява финансово, материално, инфраструктурно управление на въздушното движение и други специфични изисквания, свързани с ефективното използване на силите и средствата на операторите на въздушни средства, необходими за изпълнение на задачите.

5. Изпълнението на поетите функции или задачи се регулира нормативно в държавата. То включва контрол от държавата на планирането, подготовката и натренираността на личния състав на операторите на въздушните средства за изпълнение на поетите задължения, поддържането в постоянна готовност на силите и средствата и др. специфични изисквания.

6. Поддържането на необходимата специална и летателна подготовка и ниво на постоянна натренираност на личния състав за срочно и безопасно изпълнение на задачите за нуждите на ВИС се урежда нормативно в държавата.

Основни *функции* на ВИС:

1. Организационно-управленска функция на ВИС. Изпълнява се от национален оперативен център, който е логично да се изгради (съвмести), или се делегира на вече изградени и съществуващи структури в състава на българските Военновъздушни сили. Това няма да изисква нови организационни структури и нови щатни длъжности. Ако все пак това се наложи, то ще бъде в минимален състав.

2. Въздушна *разузнавателна* функция. На първоначалния етап се реализира по способи на въздушното разузнаване според оперативните способности на съществуващите авиационни структури в състава на ВВС, ВМС, МВР, Държавния авиационен оператор, Авиационния оператор за медицински цели и др. частни авиационни оператори. Впоследствие се развиват необходимите разузнавателни способности според теоретичния модел и на основата на съществуващия въздушен парк в държавата.

3. Въздушна *контраразузнавателна* функция. Първоначално се реализира по способи на въздушното разузнаване според способностите на съществуващите авиационни и други структури в състава на ВВС, ВМС, МВР, Държавния авиационен оператор, Авиационния оператор за медицински цели и др. частни авиационни оператори. Впоследствие се развиват необходимите контраразузнавателни способности според модела на основата на съществуващия въздушен парк в държавата.

4. Специални *функции.* Реализират се с въздушните средства на операторите на въздушни средства, организации и собственици на такива според съществуващите способности. В бъдеще се планира какви способности да се развият.

5. *Комуникационно-информационна* функция. Изгражда се на базата на съществуващата държавна, ведомствена и частна комуникационно-информационна система.

6. *Аналитична* функция. Реализира се чрез планови ежедневни (по-често при необходимост) доклади на операторите на въздушни средства от системата във ВИС, нормативно регулирани и форматирани.

След изясняване на концептуалните научнообосновани мултидисциплинарни подходи следва да се разгледат принципно способностите на въздушните средства за придобиване, обработка и доставяне на информация при криза в даден район в реално време. Според модела и необходимата по количество, пълнота и качество информация тя се доставя на държавните органи за управление при кризи в реално време – Министерския съвет, министерства, областни управления, общини и др.

Анализът на необходимите оперативни способности за придобиване на оперативна информация в реално време в доклада е ограничен в рамките на разглеждането на възможностите на въздушно базираните средства за придобиване на оперативна информация при кризи в обхвата на територията на Република България. Освен това е необходимо да се предвидят в модела и възможности за взаимодействие/обмяна на информация със съседните ни държави, както и с регионалните организации, в които Република България е член.

Авторът на доклада няма претенции за пълнота на разглеждане на темата, но счита, че базовите и основополагащи научно и мултидисциплинарно обосновани

принципи са обхванати. Генерираните концепции, визии и стратегии за изграждане на ВИС като системен елемент от *специалната рекурсивна кризисна система в* държавата са както напълно реализуеми, реалистични и концептуално обосновани от научна гледна точка, така и икономични и изгодни за реализация в държавата във финансов, материален и кадрови ракурс. Това ще повиши възможностите на страната да се справя по-ефективно с кризисни ситуации и ще изгради способностите в система, което води до повишаване на ефективността.

Благодарности и финансиране

Тази публикация е финансирана от Министерството на образованието и науката в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г. и съгласно Споразумение № Д01-74/19.05.2022 г.

Acknowledgments and funding

The report was prepared with the financial support of the National Science Program „Security and Defense“, financed by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No. 731 of 21.10.2021.

Литература

1. **Денчев,** С. и др. Управление при кризи. София: Автоказион, 2013, с. 33. ISBN 978-954-92285-2-6.
2. **Манев,** Е. Глобална, регионална и национална сигурност. София: Состтрейд, 2012, с. 32. ISBN 978-954-334-141-2.
3. **Манев,** Е. Определение за сигурност – организационно-културен подход. – В: *Юридически* сборник, том XXIII, 2016, с. 262-274. ISSN 1311-3771.
4. **Манев,** Е. Зони и нива на сигурност – хипотези. – В: *Сборник* с доклади „Четвъртата промишлена революция и Балканите“, Международна НК, ЮФ, ВСУ „Черноризец Храбър“, 2019, кн. 36, серия „Юридически науки и обществена сигурност“, с. 7-13. ISSN 1313-7263.
5. **Манев,** Е. Изграждане на авиационен капацитет за защита при бедствия и изисквания към системата за управление. – В: *Юридически* сборник на БСУ, том XXX, 2023, с. 164-172. ISSN 1311-3771.
6. **Маринов,** Р. Кризисен мениджмънт. София: „Св. Георги Победоносец“, 1999, с. 40-45.
7. **Милушев,** Л. Кризата. Управленски аспекти и възможности. Пловдив, 2008, с. 14-18.
8. **Уайт,** Л. Науката за културата. София: Наука и изкуство, 1988.

РАЗУЗНАВАТЕЛНИТЕ СТРУКТУРИ НА ЕС

проф. д-р Васил Георгиев
Висше училище по сигурност и икономика – Пловдив

EU INTELLIGENCE SERVICES

Prof. Vasil Georgiev, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Докладът изследва съществуващите разузнавателни структури на ЕС и перспективите пред задълбочаването на взаимодействието в рамките на ЕС. Докладът се фокусира върху външнополитическите и военните структури в рамките на ОВППС и ОПСО.*
Ключови думи: *Обща външна политика и политика на сигурност на ЕС; разузнаване; разузнавателен обмен*

Abstract: *The report examines the existing EU intelligence structures and the prospects for deepening cooperation within the EU. The report focuses on foreign policy and military structures within the CFSP and CSDP.*
Key words: *EU Common Foreign and Security Policy; Intelligence; Intelligence Sharing*

Въведение

Европейският съюз не разполага с централизирани разузнавателни или контраразузнавателни служби по подобие на службите на отделните държави членки. Създаването на такива служби не е предвидено като задължение в Договора за създаване на Европейски съюз (ДЕС) и в Договора за функционирането на Европейския съюз (ДФЕС). Дори и да се приеме, че няма юридическа пречка такива да бъдат създадени с акт на вторичното законодателство, в изпълнение на целите на Общата външна политика и политика на сигурност на ЕС (ОВППС) и Общата политика за сигурност и отбрана на ЕС (ОПСО), политическите съображения все още препятстват такова решение.

Целта на настоящия доклад е да изследва съществуващите разузнавателни структури на ЕС и перспективите пред задълбочаването на взаимодействието в рамките на ЕС. Докладът се фокусира върху външнополитическите и военните структури в рамките на ОВППС и ОПСО.

Извън предмета на изследване е обменът на разузнавателна информация по линия на Европол, както и механизмите на обмен на разузнавателна информация в рамките на НАТО[1] и на други партньорства, като Nine Eyes[2]. Също така извън предмета на изследване са и въпросите на сътрудничеството в митническото разузнаване [2: 89 – 104].

[1] Механизми за обмен на разузнавателна информация има и НАТО: NATO Intelligence and Security Division (NATO ISD) – отговаря за стратегическото разузнаване и анализ на заплахите; NATO Intelligence Fusion Centre (NIFC) – координира тактическото и оперативното разузнаване от националните служби.

[2] В рамките на англоезичните държави е механизмът Five Eyes (САЩ, Канада, Австралия, Обединеното кралство и Нова Зеландия), Nine Eyes (вкл. Франция, Германия, Нидерландия, Дания, Норвегия), Fourteen EYES (вкл. Белгия, Италия, Испания, Швеция), както и други механизми.

Разузнавателен капацитет на ЕС

Необходимостта от споделяне на разузнавателна информация, от една страна, от друга страна – многопластовостта на европейската архитектура на сигурност, са наложили като носеща конструкция при събирането и анализирането на информацията да се използват **националните ресурси** на държавите членки. Международните структури имат предимно координационен и аналитичен характер. Освен структури в рамките на ЕС, налице са и структури в рамките на НАТО, както и други, международни съюзнически структури, с по-тесен и интензивен характер. Тоест сътрудничеството в рамките на ЕС не е единственото, на което разчитат европейските партньори.

В ЕС в рамките на ОВППС са учредени структури, чиято функция е да анализират получената разузнавателна информация от открити източници (OSINT) и информацията, предоставена от държавите – членки на ЕС, на доброволна основа.

На първо място такава структура е Разузнавателният и ситуационен център EU IntCen. Той подпомага политическите и оперативните решения в областта на външната политика и политиката на сигурност чрез събиране, обработка и анализ на различни видове информация. Информацията, която се анализира, е получена от различни източници – сателитни и въздушни изображения, открити данни (OSINT), доклади от държавите членки и други разузнавателни материали. Центърът не събира самостоятелно разузнавателна информация, а разчита на предоставени данни от трети страни.

Друга структура е свързана с военното разузнаване, което обезпечава гражданските и военните операции и мисии по линия на Общата политика за сигурност и отбрана. За целта към Европейската служба за външни действия – Военен щаб е създадена структурата EUMS Intelligence Directorate (IntDir, Разузнавателна дирекция на Военния щаб на ЕС). Дирекцията обработва информация от различни източници – национални военни разузнавателни служби, сателитни данни, открити източници и др.

Съвместни отчети между IntCen и IntDir се произвеждат във формат, озаглавен „Единичен капацитет за анализ на разузнаването (SIAC)“.

Друга разузнавателна структура в рамките на ЕС е структурата за събиране и анализ на геопространствена информация (GEOINT) – Сателитният център на ЕС, който подпомага ОВППС и ОПСО на ЕС чрез предоставяне на анализи и продукти, базирани на сателитни данни. Сателитният център предоставя данните и на Разузнавателния и ситуационен център, който ги интегрира с други разузнавателни източници, за да подпомогне вземането на решения в рамките на ОВППС и ОПСО.

Тези структури са част от европейското разузнавателно сътрудничество, осъществявано в институционалната рамка на ЕС.

Предизвикателствата пред създаване на разузнавателна служба на ЕС

Създаването на разузнавателни служби се възприема като израз на националния суверенитет на държавите. Този национален суверенитет, разбира се, може да бъде упражняван съвместно от държавите членки и това се прави в много области, в които е постигната конвергенция в интересите на държавите (напр. в областта на търговската политика, митническия съюз [3: 57 – 66], риболова, конкуренцията, паричната политика на държавите в еврозоната и др.).

В областта на външната политика и отбраната такава конвергенция обаче е труднопостижима.

На първо място, защото всяка държава членка участва в различни неформални конструкции и групи [9: 3] (Ваймарски триъгълник, нордическа група, средиземноморски държави), които определят различното положение на държавите във формирането на европейската външна политика – различни са регионално формулираните приоритети, различни са и акцентите в тяхната геополитическа ориентация. Тези разлики създават недоверие, доколкото една разузнавателна информация е ценна, когато може да се използва от една или няколко държави, които имат споделени приоритети. Съответно, ако тя бъде използвана от държави с различаващи се или противоположни приоритети, тя ще даде предимство на държави с разнопосочни интереси – т.е. няма да създаде реално предимство на държавата, притежаваща съответната разузнавателна информация.

Разбира се, има области, в която държавите имат еднозначно сходни приоритети (тероризъм, киберсигурност, хибридни заплахи), в които тази информация може да бъде споделяна, трябва да бъде споделяна и бива споделяна. В други области (напр. военноразузнавателна информация) споделянето в рамките на 27 държави би представлявало огромен риск за нейното компрометиране и постъпване при противника [5]. При обмена на разузнавателна информация ключово е доверието, което се има за предоставяне на разузнавателната информация. Разузнавателните служби споделят антитерористична информация, доколкото тя касае **най-масовите** нива на споделяне на информация между държави и международни организации, включително и между държави, които не си сътрудничат, тъй като касае глобален проблем, по противодействието на който има широк политически консенсус, включително и между политически противници.

На второ място, различните държави членки имат различен ангажимент към европейските външнополитически инициативи. Hofmann [8] класифицира държавите – членки на ЕС, в 4 типа според различното им ниво на ангажимент и инвестиции в европейската отбрана – архитекти, брикольори, агностици и саботьори. Архитектите (напр. Франция, Германия, Полша) чертаят стратегическите политики, брикольорите участват в тях, агностиците се стремят да участват с възможно най-малко ресурси, а саботьорите се противопоставят на общите действия, позиции или политики. Тази диспозиция води до невъзможност за формиране на обща европейска политика, поради която причина европейската външна политика през последните години, особено в контекста на войната в Украйна, изоставя тромавата институционална рамка на ЕС и използва по-гъвкави формати, като международни форуми или други международни организации или конференции (Европейската политическа общност, Групата от Лондон от февруари 2025 г. и др.). Казано иначе, в настоящия момент механизмите на ЕС за осъществяване на външна политика от страна на държавите – членки на ЕС, се оказват неособено подходящ форум (за сметка на по-гъвкави и неформални инициативи). Това повдига въпроса защо да се обезпечава една неясно колко перспективна институционална структура с разузнавателна агенция.

Не на последно място, създаването на разузнавателна агенция на ЕС е начинание, изискващо огромни ресурси: изграждане на собствени разузнавателни мрежи в чужбина, създаване на технически средства за електронно наблюдение, на аналитични центрове за обработка на информация, подбор на кадри, механизъм за контрол и др. [1: 907]. При наличието на посочените по-горе различия стимулът за изграждане на разузнавателна агенция по подобие на националните е малък, а и рискът от създаване на слаба като ефективност, но скъпа като реализация агенция не е малък.

Не по-малко значим е проблемът, наречен на една от многото крилати фрази на големия римски сатирик Ювенал „quis custodiet ipsos custodes“, или „кой ще пази самите пазачи“. Проблемът с контрола над разузнавателните служби е един от най-

важните въпроси на всяка държава [4: 275 – 295]. В това отношение създаването на разузнавателна структура на европейско ниво неминуемо ще следва да даде много ясен и недвусмислен отговор, че такъв контрол ще е реален и ефективен, – освен от европейските структури (Европейската комисия, Върховния представител по ОВПСС, Европейския парламент), и от националните правителства и парламенти.

Перспективи пред разузнавателното взаимодействие в ЕС

Глобалната стратегия на ЕС от 2016 г. [7] отделя внимание на разузнавателното взаимодействие и на важността да се интегрират и координират политическата и военната разузнавателна дейност чрез съществуващия Централен анализаторски хъб (SIAC), който обединява стратегическа информация, ранно предупреждение и подробен анализ, така че да се осигури цялостна и навременна политическа и военна гледна точка. Извън това Глобалната стратегия не предвижда институционално надграждане на така съществуващата система.

Стратегическият компас от 2022 г. [6: 12, 33] също посочва засилването на разузнавателния капацитет на ЕС като един от приоритетите в рамките на SIAC и Сателитния център.

Няколко години по-късно, през 2025, ЕС се намира в уникален момент от своето развитие, за който отдавна се готви на думи, но сега ще се наложи да се подготви и на дела. Той е в ситуация, в която е длъжен да поеме отговорност за усилване на външнополитическите и военните способности на държавите членки. Провалът да използва този прозорец на възможност носи екзистенциална заплаха за съществуването на европейските държави.

Предложеният от ЕК през март 2025 г. нов механизъм на придобиване на военни способности – т.нар. „ReArm Europe/Readiness 2030“, предполага сериозно засилване на разузнавателното взаимодействие. Механизмът включва нов финансов инструмент на стойност 150 млрд. евро под формата на заеми за държавите членки, осигурени чрез общо заемане на капиталовите пазари и гарантирани от бюджета на ЕС. Тези средства са предназначени изключително за съвместно придобиване на военна техника от европейски производители с цел съвместни поръчки на способности, с цел да се постигнат икономии от мащаба, по-ниски разходи и по-голяма оперативна съвместимост между европейските армии.

Успехът на инициативата ReArm е предпоставен от по-тясното разузнавателно сътрудничество и координация между държавите членки, доколкото съвместното планиране на отбранителни способности и общите проекти предполагат споделено разбиране за заплахите и приоритетите, което изисква известен обмен на чувствителна информация и разузнавателни оценки между партньорите. За да могат две или повече държави да решат какви съвместни способности да придобият, те трябва да достигнат до споделени оценки на стратегическата нужда от тези способности, на рисковете, които тези способности ще неутрализират, и т.н. Това предполага единна ситуационна осведоменост между тях, която се постига чрез обмен на разузнавателни данни.

В допълнение към общите придобивани способности ЕС не се е отказал от амбицията да създаде общи военни структури. Задачите на такива структури ще трябва да бъдат обезпечени с разузнавателна информация, което допълнително налага засилване на разузнавателното сътрудничество в ЕС.

На следващо място, рискът от намален разузнавателен обмен със САЩ, който беше отбелязан в контекста на преговорите за войната в Украйна, също следва да действа като сигнал за ЕС да засили собственото си разузнавателно сътрудничество. След като традиционният обмен на информация с партньори като САЩ се ограничи,

държавите членки са принудени сами да намерят начини да запълнят информационната празнина – както чрез по-голяма интеграция и координация в рамките на съществуващите структури (SIAC, EU INTCEN и EUMS INT), така и чрез кадрови, юридически и институционален ъпгрейд.

Всички тези фактори в обозримо бъдеще едва ли ще доведат до създаване на разузнавателна агенция на ЕС. Създаването на такава агенция би легнало на плещите на по-силните държави членки – и организационно, и ресурсно, като същевременно е спорно дали ще добави сериозна стойност към информационния ресурс, който ще получат в замяна. От друга страна самото създаване на такава агенция би било от полза на държавите с по-малък разузнавателен капацитет, доколкото ще имат на разположение обща и солидна разузнавателна институция. Това разминаване във възможностите и нуждите на различните държави членки също ще представлява предизвикателство пред създаването на обща разузнавателна агенция на ЕС.

Не на последно място, както вече беше посочено, доверието е ключов елемент при предоставянето на разузнавателна информация. В това отношение предоставянето на разузнавателна информация на служби, които са под политическо или фактическо влияние на противници на ЕС (като Русия), е ограничено – то не включва чувствителна разузнавателна информация, която би могла да достигне до противника. Това обстоятелство също представлява сериозно предизвикателство пред реализацията на евентуална европейска разузнавателна агенция.

Заключение

Дилемата пред Европейския съюз е дали ще успее да обедини ресурсите на държавите членки, за да устои на неблагоприятните промени, или ще остане проект, отнасящ се предимно до общия пазар.

Обединяването на ресурси и създаването на разузнавателна агенция на ЕС ще доведат до засилване на разузнавателните възможности на държавите от ЕС – нещо, което е жизненонеобходимо за тяхното по-нататъшно развитие.

Основният риск пред създаването на европейска разузнавателна агенция, която и събира, и анализира разузнавателна информация, е в доверието, което разузнавателните общности на държавите членки имат помежду си, и в контрола, който ще се осъществява върху дейността на такъв тип структура. Този риск до голяма степен е труднопроследим, като се има предвид естеството на дейността на разузнаването, която дейност е преди всичко секретна.

Опасенията, че една такава разузнавателна агенция ще подрони националните държави, обаче са недобре обосновани поради поне две причини.

На първо място, държавите – членки на ЕС, и досега разчитат на партньорска разузнавателна информация, която да обезпечава външнополитическите и военните им решения.

На второ място, в областта на разузнаването повече източници на информация означава по-добре обезпечено политическо решение. Малко са държавите, които в своята национална институционална рамка разчитат само на една разузнавателна структура.

Поради тази причина създаването на пълноценна разузнавателна служба на ЕС, чиято дейност подлежи на контрол както от европейските институции, така и от националните парламенти и правителства на държавите членки, би могла да бъде подходящ инструмент както за преодоляване на дефицита на разузнавателна информация вследствие на нарушените партньорски отношения със САЩ, така и като отговор на

новите технологични предизвикателства при събирането и анализирането на разузнавателна информация.

Литература

1. **Ангаров,** Д. Въоръжени сили и разходи за отбрана. – В: *Сборник* с доклади от научната конференция „Знание, наука, технологии, иновации“, юли 2024, с. 905 – 913. ISSN (Print) 2815-3472. ISSN (CD) 2815-3480.
2. **Младенов,** И. Административни видове митнически разузнавателни процедури. – В: *Общество* и право, бр. 3, 2020, с. 89 – 104. ISSN 0204-8523.
3. **Младенов,** И. Митническото разузнаване – правни принципи, залегнали в институционалната активност на митническото разузнаване. – В: *Общество* и право, бр. 8, 2018, с. 57 – 66. ISSN 0204-8523.
4. **Born,** H. Democratic and parliamentary oversight of the intelligence services: practices and procedures. – In: *Sourcebook* on security sector reform Collection of Papers. Philipp Fluri, Miroslav Hadžić. (Eds.). Geneva/Belgrade, March 2004, pp. 275-295.
5. **Bradberry,** D. Civilian and Military Intelligence – Necessary Dichotomy. – In: *American* Diplomacy, May 2006. [online]. [available 25.03.2025]. *https://americandiplomacy.web.unc.edu/2006/05/civilian-and-military-intelligence-a-necessary-dichotomy/*.
6. **European** External Action Service. 2022. – In: *Strategic* Compass of the EU 2022. Brussels: European External Action Service, p.p. 12; 33.
7. **European** Union External Action Service. Shared Vision. Common Action: A Stronger Europe. A Global Strategy for the European Union’s Foreign and Security Policy. European Union External Action Service, 2016, т. 34.
8. **Hofmann,** S. Organizing European security in yet another geopolitical era: consensus escapism or compartmentalized multilateralism? – In: *International* Politics. [online]. [available 25.03.2025]. *https://doi.org/10.1057/s41311-024-00651-z*.
9. **Viceré,** Maria Giulia Amadio, Monika Sus. Organizing European security through informal groups: insights from the European Union’s response to the Russian war in Ukraine International Politics, 7.12.2024, p. 3. [online]. [available 25.03.2025]. *https://doi.org/10.1057/s41311-024-00657-*.

ARTIFICIAL INTELLIGENCE IN THE MODERN FINANCIAL SECURITY ENVIRONMENT

Prof. Marijana Joksimović, PhD
Alfa BK University – Belgrade, Serbia

ИЗКУСТВЕН ИНТЕЛЕКТ В СЪВРЕМЕННАТА СРЕДА ЗА ФИНАНСОВА СИГУРНОСТ

проф. д-р Марияна Йоксимович
Университет Алфа БК – Белград, Сърбия

Резюме: *В съвременната среда на финансова сигурност изкуственият интелект (ИИ) се превръща в незаменим инструмент за подобряване на управлението на риска, откриване на измами и гарантиране на цялостната стабилност на финансовите системи. Технологиите, базирани на ИИ, като машинно обучение, обработка на естествен език и анализ на данни, позволяват на финансовите институции да анализират огромни количества данни в реално време, да идентифицират модели и да прогнозират потенциални заплахи за сигурността. Тези възможности позволяват по-ефективно разкриване и предотвратяване на финансови престъпления, включително кибератаки, пране на пари и измами, като същевременно подобряват процесите на вземане на решения и спазването на нормативните изисквания. Тъй като предизвикателствата пред финансовата сигурност стават все по-сложни, ИИ не само подпомага традиционните мерки за сигурност, но и въвежда иновативни решения за проактивно намаляване на риска. Интегрирането на ИИ в системите за финансова сигурност обаче поражда и опасения, свързани с неприкосновеността на личния живот, алгоритмичната пристрастност и необходимостта от адекватни регулаторни рамки. В настоящия доклад се разглежда ролята на ИИ в трансформирането на финансовата сигурност, потенциалните ползи от него и свързаните с него предизвикателства, като се акцентира върху важността на адаптирането към развиващия се цифров пейзаж.*

Ключови думи: *изкуствен интелект; цифрови финанси; съвременна финансова сигурност; иновации; блокчейн технология; цифрови валути; финансови технологии (FinTech); технологии, базирани на изкуствен интелект*

Abstract: *In the modern financial security environment, Artificial Intelligence (AI) is becoming an indispensable tool for enhancing risk management, detecting fraud, and ensuring the overall stability of financial systems. AI-driven technologies, such as machine learning, natural language processing, and data analytics, enable financial institutions to analyze vast amounts of data in real-time, identify patterns, and predict potential security threats. These capabilities allow for more efficient detection and prevention of financial crimes, including cyber-attacks, money laundering, and fraud, while also improving decision-making processes and regulatory compliance. As financial security challenges become increasingly complex, AI not only supports traditional security measures but also introduces innovative solutions for proactive risk mitigation. However, the integration of AI into financial security systems also raises concerns related to data privacy, algorithmic bias, and the need for adequate regulatory frameworks. This abstract explores the role of AI in transforming financial security, its potential benefits, and the associated challenges, with a focus on the importance of adapting to an evolving digital landscape.*

Key words: *Artificial Intelligence; digital finance; modern financial security; innovation; blockchain technology; digital currencies; financial technologies (FinTech); AI-driven technologies*

Introduction

In recent years, Artificial Intelligence (AI) has emerged as a pivotal force driving innovation across various sectors, with finance being no exception. The increasing complexity of financial systems, combined with evolving threats in cyber security, has led to the

adoption of AI technologies to strengthen financial security frameworks. AI's potential to enhance the detection of fraud, optimize risk management, and bolster overall financial stability has attracted significant attention from financial institutions, regulatory bodies, and researchers alike.

The landscape of financial security has changed dramatically in the face of global challenges such as cybercrime, money laundering, and data breaches, leading to the need for more robust, efficient, and scalable security solutions. AI, with its ability to process vast amounts of data in real time, identify patterns, and make predictive analyses, is uniquely positioned to address these challenges. Moreover, AI tools, such as machine learning algorithms, natural language processing, and advanced data analytics, are increasingly being integrated into financial security strategies to mitigate risks and prevent financial crimes.

This paper seeks to explore the integration of AI in the modern financial security environment. By investigating its role in enhancing the security of financial systems, detecting fraudulent activities, and improving compliance with regulatory requirements, the paper aims to provide a comprehensive understanding of how AI is reshaping financial security protocols. Furthermore, it will analyze the challenges and opportunities associated with AI adoption, including concerns related to data privacy, algorithmic bias, and the need for new regulatory frameworks to accommodate emerging technologies.

To achieve this, the paper employs a qualitative and descriptive research methodology, encompassing a thorough literature review, case study analysis, expert interviews, and comparative analysis. By synthesizing existing research and real-world examples, the paper will highlight the current state of AI applications in financial security, the potential future developments, and the key factors influencing the successful integration of AI within financial institutions.

Methodology and Literature

The methodology used in this paper follows a qualitative and descriptive research approach to explore the role of Artificial Intelligence (AI) in the modern financial security environment. The study aims to examine how AI technologies are integrated into financial security systems, their impact on risk management, fraud detection, and overall stability in the financial sector.

The methodology utilized in this study combines a qualitative approach with a comprehensive review of the existing literature on AI in financial security. The research is designed to provide insights into both theoretical perspectives and practical applications of AI technologies in combating financial security risks. A comprehensive literature review is conducted to analyze existing research, reports, and case studies related to AI applications in financial security. This review provides insights into the evolution of AI in the financial sector, its current usage, and its potential to address emerging security challenges. The paper explores real-world case studies from financial institutions that have successfully implemented AI-driven technologies in their security operations. These case studies help demonstrate practical applications and the effectiveness of AI in addressing specific financial security issues, such as fraud prevention, transaction monitoring, and cyber security threats. The analysis of secondary data, including financial reports, industry surveys, and security breach statistics, allows for an assessment of the current state of AI implementation in the financial sector. Data will be gathered from industry sources such as the European Central Bank (ECB), the Bank for International Settlements (BIS), and other financial regulatory bodies. To supplement the secondary data, interviews with AI experts, financial security professionals, and regulatory authorities are conducted to gather first-hand insights into the

practical challenges and opportunities presented by AI in financial security. The study compares the use of AI across different regions and financial institutions to identify trends, best practices, and gaps in AI implementation. This analysis is critical for understanding the scalability and adaptability of AI solutions in varying financial environments.

The literature reviewed for this study includes foundational texts on AI, financial security, and the intersection of both fields. Key publications and reports from academic sources, industry organizations, and financial institutions will be analyzed to provide a comprehensive view of the current state of AI in financial security. The literature review will also serve as a foundation for understanding the potential risks and rewards associated with AI technologies in the financial sector.

By combining these methods, the paper aims to contribute to the growing body of knowledge surrounding AI's role in modern financial security, offering practical insights and recommendations for financial institutions, policymakers, and researchers.

Data in the Paper

The integration of Artificial Intelligence (AI) in financial security has become increasingly critical, with several key data points reflecting its growing importance and impact on the sector. Below are some notable statistics and trends regarding AI adoption in financial security [4].

AI Market Growth in Financial Security: According to a report by Markets and Markets (2020), the AI in the financial services market is expected to grow from $7.91 billion in 2020 to $26.67 billion by 2026, at a compound annual growth rate (CAGR) of 22.5%. This growth reflects the increased demand for AI technologies in risk management, fraud detection, and cybersecurity.

Fraud Detection and Prevention: The Association of Certified Fraud Examiners (ACFE) estimates that fraud costs the global economy more than $5 trillion annually(ACFE, 2019), a significant portion of which is preventable through AI technologies. AI systems are increasingly used to detect financial fraud. For example, 70% of financial institutions in a survey conducted by Accenture in 2019 indicated they were already leveraging AI for fraud detection, with 84% of respondents planning to implement AI-powered fraud prevention tools within the next two years.

Cybersecurity Threats and AI: The 2019 Global Cybersecurity Index (GCI) highlighted that cybercrime in the financial industry costs the global economy an estimated $600 billion each year. AI has proven to be an essential tool in detecting and mitigating cyber threats. According to a study by Juniper Research (JR, 2024), AI-based cybersecurity solutions are expected to save financial institutions more than $1.4 billion annually by 2024 by identifying cyber threats before they escalate.

Machine Learning [2] Algorithms for Transaction Monitoring: A report by Deloitte (2020) indicated that 65% of financial institutions utilize machine learning (ML) algorithms for transaction monitoring to prevent money laundering and other illicit activities. ML algorithms have been reported to improve the detection rate of suspicious activities by up to 50%, reducing false positives and improving the accuracy of fraud detection systems.

Regulatory Compliance and AI: The integration of AI also helps financial institutions with regulatory compliance. According to a survey by PwC (2020), 61% of financial institutions cited that AI significantly helps them meet regulatory compliance standards, especially with anti-money laundering (AML) and know-your-customer (KYC) regulations. The implementation of AI-based solutions reduces the compliance costs for institutions by up to 30-50% as it streamlines monitoring and reporting processes.

Adoption Rate of AI Technologies: A 2020 survey conducted by IBM on AI adoption in the financial sector revealed that 40% of financial services firms were actively deploying AI technologies, with another 40% considering its adoption within the next three years. AI-driven risk management tools are being adopted at a faster rate, with 58% of financial institutions having implemented AI to manage credit risk, market risk, and operational risk.

Public Perception and Concerns: A 2021 study by Accenture showed that 72% of consumers were concerned about the privacy implications of AI technologies in financial institutions, with a particular focus on data security and the potential misuse of personal information. Furthermore, 50% of financial executives expressed concerns about the lack of comprehensive regulations for AI, particularly in data protection and algorithmic transparency.

These data points illustrate the growing adoption and reliance on AI technologies to enhance financial security, along with the challenges that come with integrating such advanced systems into the financial ecosystem. Financial institutions are increasingly leveraging AI to detect fraud, reduce risks, and improve compliance, while also facing the need for appropriate regulations to mitigate potential risks related to privacy and bias in AI algorithms.

By including these data-driven insights, the paper can provide concrete evidence of AI's role in transforming the financial security landscape, helping readers understand both the current impact and future potential of AI technologies in financial systems.

AI Technologies Applied in Financial Security: Machine Learning (ML), Natural Language Processing (NLP), Robotic Process Automation (RPA) and Neural Networks and Deep Learning.

Supervised Learning: Algorithms that are trained on labeled data to make predictions, useful for detecting fraud patterns in transactions. Unsupervised Learning: Methods that analyze data without pre-labeled training, useful for anomaly detection (e.g., identifying previously unknown types of fraud). Reinforcement Learning: A model where algorithms learn to make decisions by interacting with the environment and receiving feedback (used in risk management). AI-powered NLP is used in analyzing vast amounts of unstructured data (e.g., emails, financial news, social media) for real-time risk assessment and sentiment analysis. RPA helps automate routine financial tasks, such as compliance monitoring and transaction reconciliation, thus reducing human error and improving security. Deep learning is used in detecting more sophisticated types of financial crimes by analyzing complex data patterns in large datasets.

Applications of AI in Financial Security: Fraud Detection and Prevention, AI in Real-time Fraud Monitoring: AI helps monitor transactions and detect anomalies that deviate from normal behavior. Machine learning models learn from historical fraud data to predict and prevent future fraudulent activities in real-time. Risk Management and Assessment: AI models are used to assess market risks, credit risks, and operational risks. Financial institutions use AI to predict market downturns and volatility, and assess borrower default risk based on various data inputs. Cybersecurity: Financial institutions are increasingly relying on AI to enhance their cybersecurity systems. AI-powered systems detect and neutralize threats such as malware, phishing attacks, and unauthorized access in real-time. Regulatory Compliance: AI can automate KYC (Know Your Customer) and AML (Anti-Money Laundering) procedures by verifying client information, tracking suspicious activities, and helping institutions comply with regulatory frameworks. Customer Authentication and Identity Verification: AI improves the security of customer authentication through biometric systems, including facial recognition, voice recognition, and fingerprint scanning.

AI has become a critical tool for modern financial security, offering unparalleled capabilities in fraud detection, risk management, cybersecurity, and regulatory compliance. While there are significant benefits, such as enhanced efficiency and cost reduction, there are also challenges related to data privacy, ethical considerations, and the high costs of implementation. The future of AI in financial security appears promising, with continuous advancements in predictive analytics, blockchain integration, and more personalized security solutions on the horizon.

Conclusion

The integration of Artificial Intelligence (AI) into the modern financial security environment has proven to be a game-changer for the financial industry. AI technologies are increasingly being leveraged to combat a wide array of security challenges, including fraud detection, risk management, regulatory compliance, and cyber security threats. Through advanced techniques such as machine learning, natural language processing, and data analytics, AI is enabling financial institutions to enhance their operational efficiency, identify suspicious activities in real time, and make more informed decisions.

The benefits of AI in financial security are undeniable. AI-powered systems are helping financial institutions detect and prevent fraud, protect sensitive data, and ensure compliance with complex regulatory frameworks. By automating routine processes and improving the accuracy of security measures, AI is driving down costs and reducing the number of false positives in transaction monitoring, ultimately improving the security and trustworthiness of the financial system.

However, the adoption of AI also raises significant challenges. Concerns about data privacy, algorithmic biases, and the potential for AI-driven decision-making to lack transparency must be carefully managed. Furthermore, as AI technologies continue to evolve, there is a growing need for regulatory bodies to establish clear guidelines and frameworks that ensure the responsible use of AI while protecting consumers and financial institutions alike.

Despite these challenges, the future of AI in the financial security environment appears promising. As AI capabilities continue to advance, the potential for further enhancing financial security grows. Financial institutions that embrace AI technologies will be better positioned to adapt to evolving threats, improve customer experiences, and remain competitive in an increasingly digital world.

In conclusion, AI is not only transforming the way financial institutions approach security but is also shaping the future of the financial industry itself. By embracing these technologies, while addressing the associated risks, the financial sector can enhance its resilience and continue to thrive in an increasingly complex global environment. The ongoing collaboration between financial institutions, regulators, and technology developers will be crucial in ensuring that AI's integration into financial security is both effective and ethical.

This paper is part of the research results on Project U 01/2023 Green economy in the era of digitization and Project U 01/2024 Sustainable development and environmental protection in economy, Faculty of Finance, Banking, and Auditing, Alfa BK University.

Literature

1. **Arner,** D. W., J. Barberis & R. P. Buckley. (2017). FinTech, RegTech, and the Reconceptualization of Financial Regulation. – In: *Northwestern* Journal of International Law & Business, 37(3), p.p. 371-413.
2. **Brynjolfsson,** E. & A. McAfee. (2017). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.

3. **Chen,** M., S. Mao & Y. Liu. (2014). Big Data: A Survey. – In: *Mobile* Networks and Applications, 19(2), p.p. 171-209.
4. **Gartner,** Inc. (2020). Artificial Intelligence in Financial Services: The Key Trends Shaping the Future of Financial Security. Gartner Research.
5. **KPMG.** (2020). The Future of Financial Services: AI and Data-Driven Risk Management. KPMG Insights.
6. **Peters,** A. M. (2019). AI and the Financial Industry: The Changing Face of Financial Security. Springer International Publishing.
7. **Susskind,** R. & D. Susskind. (2015). The Future of the Professions: How Technology Will Transform the Work of Human Experts. Oxford University Press.
8. **Zohdy,** M. A. & M. M. El-Masri. (2020). Artificial Intelligence for Financial Fraud Detection: A Review. – In: *Journal* of Financial Technology, 2(1), p.p. 10-25.

СТРАТЕГИЧЕСКОТО РАЗУЗНАВАНЕ В СЪВРЕМЕННАТА СРЕДА НА СИГУРНОСТ

доц. д-р Тодор Димитров
Военна академия „Г. С. Раковски“ – София

STRATEGIC INTELLIGENCE IN THE MODERN SECURITY ENVIRONMENT

Captain 1st rank Assoc. Prof. Todor Dimitrov, PhD
G. S. Rakovski National Defence College – Sofia

Резюме: *Настоящият доклад изследва стратегическото разузнаване (СР) в съвременната среда на сигурност, като разглежда неговото значение, предизвикателства и бъдещи перспективи. Анализирани са ключови теоретични основи, ролята на СР в политиките за сигурност, както и примери, които подчертават успехите и провалите в разузнавателната област. Акцентира се на възникващите заплахи, технологичните иновации и необходимостта от международно сътрудничество. Докладът предлага препоръки за подобряване на разузнавателните способности.*

Ключови думи: *стратегическо разузнаване; сигурност; киберсигурност; изкуствен интелект*

Abstract: *This report examines strategic intelligence in the modern security environment, focusing on its significance, challenges, and future perspectives. It analyzes key theoretical foundations, the role of strategic intelligence in security policies, and historical case studies highlighting successes and failures in intelligence operations. Special attention is given to emerging threats, technological advancements, and the necessity of international cooperation. The report provides recommendations for enhancing intelligence capabilities.*

Key words: *strategic intelligence; security; cybersecurity; artificial intelligence*

Въведение

Стратегическото разузнаване (СР) играе ключова роля в оформянето на политиките за национална сигурност и осигуряването на ефективно взимане на решения във все по-сложен глобален контекст [16]. То представлява систематичен, целенасочен и многоаспектен процес, който обхваща добиването и анализа на стратегическа разузнавателна информация, както и своевременното ѝ предоставяне на съответните потребители в изпълнение на поставените разузнавателни задачи. СР осигурява държавното и военното ръководство с разузнавателна информация, необходима за дейността им за формиране на политиката за национална сигурност, отбранителната политика, изпълнението на задълженията към НАТО и ЕС, както и за изграждането и подготовката на ВС на страната [1]. За разлика от тактическото или оперативното разузнаване, които се фокусират върху непосредствени или краткосрочни задачи, СР предоставя по-широка, задълбочена и дългосрочна перспектива. То се отнася до систематичното добиване на данни, трансформирането им в анализирана и релевантна информация, която подпомага взимането на решения на високо ниво в областта на националната сигурност, военните операции и международните отношения [4]. Чрез интегриране на множество източници на информация от икономическата, политическата, военната и технологичната сфера СР подпомага взимането на информирани и проактивни решения [17].

Историческото развитие на СР датира още от древните цивилизации, когато военни и държавни лидери разчитат на информатори, разузнавачи и разузнавателни мисии, за да събират информация за своите противници. В своя трактат „Изкуството на войната“ Сун Дзъ определя разузнаването като ключов инструмент за постигане на победа без бой, чрез познаване на врага, себе си и обстоятелствата, което позволява стратегическо предимство и минимизиране на загубите [2]. През XX и XXI в. СР се развива значително, включвайки усъвършенствани технологични инструменти, като сателитни изображения, кибернаблюдение и анализи, базирани на изкуствен интелект (ИИ) [16]. Разузнавателната еволюция трансформира начина, по който политическите и военните ръководства оценяват заплахите, прогнозират поведението на противниците и разработват дългосрочни стратегии за сигурност.

В съвременната среда на сигурност СР е от съществено значение за справянето с глобални предизвикателства, като геополитическо напрежение, тероризъм, киберзаплахи и нововъзникващи технологични разработки [6]. Правителствата и разузнавателните служби разчитат на СР за: идентифициране и неутрализиране на потенциални заплахи за сигурността, преди те да ескалират; усъвършенстване на отбранителния капацитет и стратегическото планиране на отбраната; подкрепа на дипломатическите преговори и международното сътрудничество; укрепване на киберсигурността за защита на критичната инфраструктура; предоставяне на анализи на икономическото и технологичното развитие, които могат да окажат влияние върху националната сигурност [17].

Настоящият доклад има за цел да изследва значението, тенденциите и предизвикателствата за СР в контекста на съвременната среда на сигурност. Анализът обхваща теоретичните основи и историческата еволюция на СР, неговото място в националните стратегии за сигурност и ролята му в международните отношения. Акцент е поставен върху нововъзникващи тенденции, включително прилагането на ИИ и анализ на големи масиви от данни. Чрез комбиниране на историческа ретроспекция със съвременни изследвания се цели изграждането на цялостно разбиране за същността и значението на СР в контекста на глобалната сигурност.

Теоретични основи на стратегическото разузнаване

Концепцията за СР се е развивала в продължение на векове, като нейните корени могат да бъдат проследени в ранните военни и политически стратегии. Исторически събирането на разузнавателна информация често е било извършвано чрез шпионаж, дипломатически пратеници и разузнавателни мисии на бойното поле. Древни цивилизации, като елинската, римската и др., са използвали разузнаването, за да си осигурят военно предимство [12]. Стратегът Сун Дзъ подчертава значението на разузнаването във военните действия – принцип, който остава актуален и в съвременните изследвания в сферата на сигурността. Институционализацията на разузнавателните агенции през XX в., особено по време на Студената война, бележи значителен поврат в практиките на СР. Държавите създават специализирани разузнавателни служби за наблюдение на противниците и прогнозиране на глобалните тенденции в сигурността [16].

Няколко ключови теории и модели формират основата на СР: Моделът на разузнавателния цикъл е широкоизползвана рамка, която очертава процеса на събиране, обработка, анализ, разпространение на разузнавателната информация, както и обратна връзка [6]. Този модел осигурява структурирани подходи към разузнавателната дейност, позволявайки непрекъснато усъвършенстване въз основа на реални събития. Друга ключова теоретична перспектива е теорията за рационалния избор, която предполага, че разузнавателните служби действат като рационални субекти, анализирайки

разходите и ползите с цел оптимизиране на решенията в областта на националната сигурност [10]. Теорията за обработката на информация разглежда как разузнавателните служби управляват огромни масиви данни, филтрират релевантната информация и извеждат приложими анализи [14].

В разузнавателните изследвания се установява основно разграничение между стратегическото, оперативното и тактическото разузнаване. Докато тактическото разузнаване се фокусира върху непосредствени заплахи и бойни операции, а оперативното разузнаване служи като мост между краткосрочните и средносрочните решения, СР има по-широка и дългосрочна насоченост. То информира висшите политически и военни стратези, като спомага за формирането на външната политика, отбранителното планиране и доктрините за сигурност [27]. Това разграничение е от решаващо значение за разбирането на начина, по който разузнавателните служби разпределят ресурсите и приоритизират разузнавателните задачи в различните направления.

Ролята на стратегическото разузнаване в съвременната среда на сигурност

СР играе жизненоважна роля в оформянето на политиките за национална сигурност, военните стратегии и международните отношения. Разузнавателните служби работят за прогнозиране на потенциални заплахи за сигурността, извършват анализ на геополитическата среда и оценяват стабилността на отделни държави и региони. В условията на все по-взаимнозависим и глобализиран свят разузнавателната дейност не се ограничава само до традиционните военни заплахи, а включва също аспекти, като икономическа сигурност, управление на енергийните ресурси, екологически рискове и предизвикателства, свързани със здравната сигурност [27].

Икономическото разузнаване се е утвърдило като съществен компонент на стратегическото разузнаване, тъй като държавите се стремят да защитят своите икономически интереси от кражба на интелектуална собственост, кибериконomически шпионаж и търговски манипулации [8]. В условията на нестабилна глобална среда правителствата и корпорациите все по-често разчитат на разузнавателни оценки за ограничаване на рисковете на международните пазари и предвиждане на промени в икономическата динамика. В епохата на икономическото противопоставяне разузнавателните служби анализират валутните колебания, търговските споразумения и уязвимостите във веригите за доставки с цел защита на националните интереси [4].

Друг съществен аспект на СР е борбата с тероризма и трансграничната организирана престъпност. Разузнавателните агенции проследяват дейността на глобалните престъпни мрежи, участващи в трафика на наркотици, търговията с хора и незаконната търговия с оръжие [23]. Тези мрежи често се възползват от слабите механизми за управление в определени региони, което прави координацията между държавите от съществено значение за разграждането на престъпните организации.

Основни предизвикателства в стратегическото разузнаване

Наред с огромното си значение и важните задачи, които решава, СР е изправено и пред редица предизвикателства, които затрудняват неговата ефективност. Един от най-големите проблеми е нарастващата сложност на глобалната среда за сигурност. Преходът от конвенционална война към мултидомейнови операции в съчетание с нарастващ дял на асиметричните заплахи, като кибератаки и терористични мрежи, прави събирането на разузнавателна информация по-трудно [29]. Тези заплахи често нямат ясна държавна принадлежност, което затруднява тяхното проследяване и неутрализиране.

Друго предизвикателство е политизирането на разузнаването. Разузнавателните оценки понякога могат да бъдат повлияни от политически интереси, което води до пристрастно докладване и неправилни решения [9]. Натискът за съгласуване на разузнавателните оценки с политическите цели може да подкопае обективността и точността на разузнавателния анализ. Гарантирането на независимостта и аполитичността на разузнаването е от решаващо значение за поддържане на неговата надеждност и ефективност.

Технологичният напредък носи както възможности, така и уязвимости. Докато ИИ и машинното обучение подобряват обработката на разузнавателна информация, те също така въвеждат рискове, свързани с алгоритмични пристрастия и прекомерна зависимост от автоматизирани системи [24]. Същевременно киберзаплахите продължават да нарастват, като застрашават все повече класифицираната разузнавателна информация. Необходимо е разузнавателните агенции непрекъснато да адаптират своите мерки за киберсигурност, за да защитят чувствителната информация от кибератаки.

Предизвикателство представлява и обменът на разузнавателна информация между националните служби и съюзническите държави. Въпреки че сътрудничеството засилва глобалните усилия за сигурност, разликите в националните приоритети, правните рамки и доверието между разузнавателните служби могат да възпрепятстват ефективния обмен на информация. Установяването на сигурни и стандартизирани споразумения за споделяне на разузнавателна информация е от съществено значение за подобряване на многонационалното разузнавателно сътрудничество [19].

Стратегическото разузнаване се влияе не само от технологични и оперативни фактори, но и от когнитивни и аналитични подходи. Анализаторите прилагат структурирани аналитични техники (SATs), като анализ на сценарии, „червен екип“ (red teaming) и конкурентен анализ, с цел повишаване на точността и обективността на оценките [12]. В същото време когнитивните изкривявания, включително склонността към потвърждение (confirmation bias) и груповото мислене (groupthink), създават предизвикателства за качеството на разузнавателната продукция. Това налага систематично обучение и прилагане на методологични механизми за ограничаване на грешките в преценката [13]. Продължаващото развитие на аналитичните практики играе съществена роля за ефективността на стратегическите разузнавателни дейности в глобален мащаб.

Тенденции и бъдещи перспективи

Областта на СР продължава да се развива под въздействието на нововъзникващи заплахи, ускорени технологични иновации и динамични геополитически промени. Сред ключовите тенденции се откроява засиленото прилагане на ИИ и машинно обучение в процесите на събиране, анализ и обработка, както и при взимането на стратегически решения, подкрепени от разузнавателни оценки [22]. Системите, базирани на ИИ, могат да обработват огромни количества данни със скорости, далеч надхвърлящи човешките възможности, което позволява на разузнавателните агенции да идентифицират модели, да откриват аномалии и да генерират прогнозни оценки с по-висока точност. Алгоритмите за машинно обучение усъвършенстват разузнавателния анализ чрез способност за адаптивно обучение от нови източници на данни, като по този начин спомагат за ограничаване на човешките грешки и намаляване на влиянието на когнитивните изкривявания в аналитичния процес [29].

Киберсигурността се превърна в неразделна част от СР. С нарастващата сложност на киберзаплахите разузнавателните агенции разработват усъвършенствани ки-

берразузнавателни способности за противодействие на държавно спонсорирани хакерски атаки, кибершпионаж и рансъмуер атаки [18]. Разпространението на дийпфейк технологии и кампании за дезинформация също представлява сериозна заплаха, което изисква разузнавателните служби да инвестират в дигитална криминалистика и инструменти за проверка на достоверността, за да се справят с манипулираната информация [26].

Друга ключова тенденция е разширяването на космическото разузнаване. Сателитното разузнаване, геопространственото разузнаване (GEOINT) и възможностите за наблюдение в реално време се използват все по-често за следене на военни дейности, проследяване на нелегални мрежи за трафик и реагиране на екологични и хуманитарни кризи [3]. Миниатюризацията на сателитите и възходът на частния космически сектор разширяват достъпа до разузнавателни данни в реално време, повишавайки ситуационната осведоменост на агенциите за национална сигурност [21].

Интеграцията на квантовите изчисления в разузнавателните операции представлява едновременно възможност и риск. Квантовото криптиране обещава безпрецедентна сигурност за класифицираните комуникации, но в същото време квантовото декриптиране може да представлява значителна заплаха за съществуващите криптографски протоколи, което прави разузнавателните данни уязвими [7]. За да защитят операциите си от бъдещите квантови изчислителни технологии, разузнавателните агенции трябва да инвестират в квантово устойчиви криптографски решения.

Възходът на разузнаването от открити източници (OSINT) също променя начина, по който се осъществяват стратегическите разузнавателни операции. Публично достъпната информация от социалните медии, новинарските репортажи, академичните публикации и сателитните изображения са се превърнали в ключови ресурси за разузнавателния анализ. OSINT позволява извличане на информация в реално време за геополитически събития, зони на конфликти и възникващи заплахи за сигурността. Основно предизвикателство остава верификацията на достоверността и автентичността на OSINT данните, тъй като враждебни субекти все по-често манипулират цифровите платформи, за да разпространяват дезинформация и да изкривяват разузнавателните оценки. Пример за такова действие е манипулирането на изходните данни на ИИ (AI data poisoning).

Засиленият акцент върху обмена на разузнавателна информация и международното сътрудничество е друга определяща тенденция в СР. С оглед на трансграничния характер на съвременните заплахи за сигурността разузнавателните агенции създават съвместни работни групи и многонационални споразумения за обмен на разузнавателна информация, за да подобрят колективната сигурност. Организации, като НАТО, Европейския съюз и Five Eyes Alliance, улесняват обмена на данни в реално време, подобрявайки способността на държавите да предвиждат и реагират на глобални заплахи за сигурността.

Исторически паралели и съвременни казуси

Изследването на исторически и съвременни разузнавателни операции предоставя ценни уроци за силните и слабите страни на СР. Един от най-успешните примери в съвременната история е мисията на американските разузнавателни служби, довела до елиминирането на Осама бин Ладен през 2011 г. [5]. Операцията демонстрира ефективността на интегрирането на различни подходи, включително разузнаване чрез човешки източници (HUMINT), сигнално разузнаване (SIGINT), геопространствено разузнаване (GEOINT) и киберразузнаване (CYBINT). Значителното време, отделено за разузнаване и проникване в мрежите на терористичната организация, позволява на специалните

части на американските военноморски сили (U.S. Navy SEALs) да извършат прецизна и успешна операция в комплекса на Бин Ладен в Аботабад, Пакистан [25].

Един от емблематичните разузнавателни успехи е разшифроването на германската криптираща машина „Енигма“ от британските разузнавателни служби по време на Втората световна война. Декодирането на нацистките комуникации дава решаващо предимство на съюзниците и променя хода на войната. Въпреки успеха си съюзниците са принудени да запазят тайната, като в някои случаи умишлено позволяват атаки срещу собствени кораби, за да не разкрият декодирането на германските комуникации [11].

Друг казус, който подчертава значението на СР, е Карибската криза от 1962 г. По време на тази конфронтация разузнавателните служби на САЩ изиграват ключова роля в разкриването на съветските ракетни установки в Куба чрез въздушно разузнаване и сателитни изображения [20]. Разузнавателните оценки предоставят на американските лидери необходимите данни за формулирането на дипломатическа стратегия, която в крайна сметка води до мирно разрешаване на конфликта и предотвратяване на ядрена война [19].

Пример за ефективно СР е операция „Орхидея“, при която Израел извършва превантивен въздушен удар срещу иракския ядрен реактор „Озирак“ през 1981 г. Израелското разузнаване успешно разкрива ядрените амбиции на Саддам Хюсеин, проследява френските ядрени инженери, работещи в Ирак, и използва сателитни изображения за потвърждаване на събраната информация. Въпреки военния успех операцията предизвиква международни дебати и напрежение в Близкия изток [15].

От друга страна разузнавателните провали също са изиграли роля в развитието на СР. Един от най-известните примери е атаката срещу Пърл Харбър през 1941 г. Въпреки наличието на разузнавателни сигнали за предстояща атака американските разузнавателни служби не успяват да ги анализират правилно, което води до неподготвеност при нападението на японските военноморски сили. Друг класически разузнавателен неуспех е неточната интерпретация на разузнавателните данни, довела до инвазията в Ирак през 2003 г. Разузнавателните агенции погрешно заключават, че Ирак притежава оръжия за масово унищожение, което води до военна интервенция със сериозни геополитически последици. Този случай подчертава опасностите от когнитивни предразсъдъци, политизацията на СР и липсата на критична оценка на източниците [13].

Един от съвременните примери за провал на разузнаването е използването от Китай на комбинация от традиционни разузнавателни методи и кибершпионаж за придобиване на икономически и военни технологии. Операцията „APT10“ през 2018 г. компрометира американски, японски и европейски компании, извличайки чувствителна информация. Чрез техника, известна като „cloud-hopping“, атакуващите получават достъп до данни на множество компании, включително от сектори, като авиация, фармация, отбрана и технологии. Западните държави впоследствие предприемат мерки за ограничаване на китайското кибервлияние, включително санкции срещу китайски технологични компании и засилване на контраразузнавателните механизми [28]. Операцията разкрива уязвимостите на глобалната информационна инфраструктура и подчертава ролята на киберпространството като арена за СР. Демонстрира се как държавно спонсорирани групи могат да използват частния сектор като посредник за разузнаване.

Друг значим пример е руската инвазия в Украйна през 2022 г., при която руските разузнавателни служби погрешно оценяват способността на Украйна да се съпротивлява и подценяват реакцията на Запада. Неточните разузнавателни доклади водят до очаквания за бърза победа, която не се осъществява, а в резултат на неправилния анализ руската военна кампания среща неочаквано силна съпротива. От своя

страна западните разузнавателни служби успяват да предвидят руската инвазия месеци преди да се случи, което позволява превантивни военни и дипломатически реакции. Обменът на разузнавателна информация между съюзниците в НАТО изиграва важна роля за отбранителната стратегия на Украйна, подчертавайки значението на разузнаването в реално време за определяне на изхода на бойните действия.

Международните примери подчертават ролята на стратегическото разузнаване, чийто успех зависи от технологии, инфилтрация и анализ, а провалите – от грешки и подценяване.

Заключение и препоръки

С усложняването на заплахите СР остава основен елемент на националната и глобалната сигурност. Разузнавателните служби трябва непрекъснато да адаптират своите методологии, инструменти и стратегически перспективи, за да останат ефективни. Изводите от настоящото изследване подчертават критичната роля на СР за предвиждане на заплахите за сигурността, подпомагане на политическите решения и защита на националните интереси.

Една от основните области за усъвършенстване е инвестирането в технологични нововъведения. От първостепенна важност са интеграцията на ИИ, машинното обучение и анализ на големи бази данни в разузнавателните операции. Тези технологии могат значително да повишат акуратността и бързината на разузнавателния процес, като позволят обработка и обмен на значителни обеми данни в реално време. Първостепенно направление е развитието на киберсигурността. Все по-актуално е разработването на усъвършенствани механизми от разузнавателните служби за защита на класифицираната информация от киберпроникване и хакерски атаки.

Важна насока е подобряването на междуинституционалния и международния обмен на разузнавателна информация. Като се има предвид, че тероризмът, киберпрестъпността и геополитическите конфликти надхвърлят националните граници, е все по-важно разузнавателните агенции да засилят сътрудничеството на национално ниво и с държавите съюзници. Етичните съображения също остават от съществено значение. Докато разузнаването трябва да се фокусира върху националната сигурност, е необходимо също да се спазват демократичните ценности и принципите на правата на човека.

Друга първостепенна препоръка е развитието на квалифициран персонал в разузнавателните служби. Инвестициите в целенасочено и непрекъснато обучение, обхващащо структурирани аналитични техники, разпознаване на когнитивни изкривявания и изграждане на способности за прогнозиране, са от съществено значение за укрепване на разузнавателния капацитет. Изграждане на интердисциплинарен подход в обучението, който да включва познания за съвременните технологии, езикова подготовка, културна осведоменост и етика на разузнаването. Необходимо е също така развиване на практически умения чрез симулации, казуси и съвместни учения с други структури с цел адаптивност към динамичната среда на сигурността и новите хибридни заплахи. Значима насока за усъвършенстване е разузнавателните агенции да инвестират в борбата срещу дезинформацията. С нарастващата роля на информационните операции е необходимо разработването на инструменти за откриване и противодействие на враждебни кампании в социалните медии.

В обобщение, бъдещето на СР ще зависи от способността на разузнавателните служби да се адаптират към технологичните иновации, да се справят с нововъзникващите заплахи и да използват успешно междуведомственото и международното сътрудничество.

Литература

1. **Димитров,** Т. (2020). Разузнаването като инструмент на стратегията. – В: *Сборник* с доклади НВУ, с. 1255 – 1263. ISSN 2367-7481.
2. **Сун Дзъ.** (2003). Изкуството на войната. София: Фама.
3. **Banasik,** M. (2021). Hybrid Threats and Hybrid Warfare: The Future of Warfare? – In: *Defense* & Security Analysis, 37(1), 1-17.
4. **Betts,** R. K. (2015). American Force: Dangers, Delusions, and Dilemmas in National Security. Columbia University Press.
5. **CIA** Historical Review Panel. (2020). Operation Neptune Spear: The Hunt for Osama bin Laden.
6. **Clark,** R. M. (2019). Intelligence Analysis: A Target-Centric Approach (5th ed.). CQ Press.
7. **Council** on Foreign Relations. (2021). Intelligence Reform in the 21st Century.
8. **Dulles,** A. (2016). The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World. Lyons Press.
9. **Fingar,** T. (2011). Reducing Uncertainty: Intelligence Analysis and National Security. Stanford University Press.
10. **Gill,** P., S. Marrin & M. Phythian. (2008). Intelligence Theory: Key Questions and Debates. Routledge.
11. **Gladwin,** L. Alan Turing, Enlgma, and the breaking of German machine ciphers in World War II. [online]. [accessed 2025/03/21]. *https://www.archives.gov/files/publications/prologue/1997/fall/turing.pdf.*
12. **Heuer,** R. J. (1999). Psychology of Intelligence Analysis. Center for the Study of Intelligence, CIA.
13. **Jervis,** R. (2010). Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War. Cornell University Press.
14. **Johnston,** R. (2005). Analytic Culture in the US Intelligence Community: An Ethnographic Study. Center for the Study of Intelligence.
15. **Kirschenbaum,** J. (2010). Operation Opera: an Ambiguous Success. – In: *Journal* of Strategic Security, Vol. III, Issue 4, 2010, pp. 49-62. eISSN: 1944-0472 49.
16. **Lowenthal,** M. (2022). Intelligence: From Secrets to Policy (9th ed.). CQ Press.
17. **National** Intelligence Council. (2021). Global Trends 2040: A More Contested World. Office of the Director of National Intelligence (ODNI).
18. **National** Security Agency (NSA). (2022). Emerging Cyber Threats and Trends.
19. **Omand,** D. (2010). Securing the State. Hurst & Company.
20. **Prados,** J. (2006). Safe for Democracy: The Secret Wars of the CIA. Ivan R. Dee.
21. **RAND** Corporation. (2022). The Future of Intelligence Analysis: Challenges and Opportunities.
22. **Rid,** T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
23. **Rovner,** J. (2011). Fixing the Facts: National Security and the Politics of Intelligence. Cornell University Press.
24. **Singer,** P. W. & E. Brooking. (2018). LikeWar: The Weaponization of Social Media. Houghton Mifflin Harcourt.
25. **Tenet,** G. (2007). At the Center of the Storm: My Years at the CIA. HarperCollins.
26. **The** White House. (2021). National Artificial Intelligence Initiative Act Report.
27. **Treverton,** G. F. (2015). National Intelligence and Science: Beyond the Great Divide in Analysis and Policy. Oxford University Press.
28. **US** Department of Justice (2018). Two Chinese Hackers Associated With the Ministry of State Security. [online]. [accessed 2025/03/21]. *https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.*
29. **Zegart,** A. (2022). Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University Press.

CHALLENGES OF APPLYING ARTIFICIAL INTELLIGENCE IN BUSINESS IN SERBIA

Assoc. Prof. Lidija Madžar, PhD
Assist. Miloš Todorov, PhD
Alfa BK University – Belgrade, Serbia

ПРЕДИЗВИКАТЕЛСТВА ПРИ ПРИЛАГАНЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В БИЗНЕСА В СЪРБИЯ

доц. д-р Лидия Маджар
ас. д-р Милош Тодоров
Университет Алфа БК – Белград, Сърбия

Abstract: *Artificial intelligence (AI) has a huge potential in various aspects of our modern personal and business life, changing the way we live, act, analyse data, think, decide and draw conclusions. AI brings numerous benefits to contemporary society, by enhancing business functions, improving business results and consumer satisfaction, facilitating data analysis and automating business processes. However, the use of AI also brings a number of challenges and obstacles, which raise numerous ethical implications and call into question the credibility of its use. In addition to the AI shortcomings and limitations, this article also analyses the state and scope of its using in the Serbian business sector with the purpose of providing a deeper insight into these important issues. Despite the proactive attitude of the Serbian Government towards the AI adoption at the national level, in Serbia the application of AI technologies in the business sector is still in its infancy. Although the country has great potential for the growth of the use of AI systems, especially in traditional industries, it is necessary to invest additional efforts in education, human capital development, automation of business processes and strategic investments as key factors for the expansion of the use of AI technologies. In Serbia, a small number of companies still use AI technologies, while they are more present in large and medium-sized companies, as well as in ICT, professional, scientific, innovation and technical activities. Bearing in mind the numerous AI-related challenges faced by companies in Serbia, it is necessary to develop adequate legal solutions that will insist on encouraging trust, reliability and safety of the use of AI, but also on protecting data privacy.*

Key words: *artificial intelligence (AI); data privacy protection; Serbia; trust; safety of AI use*

Резюме: *Изкуственият интелект (ИИ) има огромен потенциал в различни аспекти на съвременния ни личен и бизнес живот, променяйки начина, по който живеем, действаме, анализираме данни, мислим, решаваме и правим заключения. ИИ носи множество ползи за съвременното общество, като подобрява бизнес функциите, бизнес резултатите и удовлетвореността на потребителите, улеснява анализа на данни и автоматизира бизнес процесите. Използването на ИИ обаче носи и редица предизвикателства и препятствия, които пораждат множество етични последици и поставят под въпрос надеждността на използването му. В допълнение към недостатъците и ограниченията на ИИ този доклад също анализира състоянието и обхвата на използването му в сръбския бизнес сектор с цел предоставяне на по-задълбочен поглед върху тези важни въпроси. Въпреки проактивното отношение на сръбското правителство към приемането на ИИ на национално ниво в Сърбия прилагането на ИИ технологии в бизнес сектора е все още в начален стадий. Въпреки че страната има голям потенциал за нарастване на използването на ИИ системи, особено в традиционните индустрии, е необходимо да се инвестират допълнителни усилия в образованието, развитието на човешкия капитал, автоматизацията на бизнес процесите и стратегическите инвестиции като ключови фактори за разширяване на използването на ИИ технологии. В Сърбия малък брой компании все още използват ИИ технологии, докато те присъстват повече в големи и средни компании, както и в ИКТ, професионални, научни, иновационни и технически дейности. Имайки предвид*

многобройните предизвикателства, свързани с ИИ, пред които са изправени компаниите в Сърбия, е необходимо да се разработят адекватни правни решения, които да настояват за насърчаване на доверието, надеждността и безопасността на използването на ИИ, но също и за защита на поверителността на данните.

Ключови думи: *изкуствен интелект (ИИ); защита на личните данни; Сърбия; доверие; безопасност при използване на ИИ*

Introduction

As a technology that mimics human intelligence, artificial intelligence (AI) has found its enormous application in various forms and fields of the modern business environment. AI has revolutionized the flows of our private and business activities, changing the way we live, act, analyse data, think, make decisions and draw conclusions. As such, AI brings numerous benefits to modern society, by enhancing business functions, improving business results and consumer satisfaction, facilitating data analysis, and automating business processes. In this sense, AI today has a special impact on accounting and finance, content creation, improvement of customer service and support, personalization of user experience, application and optimization of information technologies (IT), on cyber security, development of human capital, legal aspects of business, sales and marketing, informed decision-making, as well as on the management of value and supply chains, shaping current jobs, workforce, companies and industries [4]. The AI mode of use in modern business is colorful and diverse, ranging from machine learning, big data analytics and cognitive technologies, all the way to deep learning and computer vision for optimizing business operations and outcomes.

Dating back to the middle of the 20th century, when inventors and scientists began to explore the possibilities of creating machines that would simulate human intelligence, AI facilitates the human daily life and work, reduces the efforts in finding ideal solutions, and increases the precision of business tasks and goals. Recently, the importance of various AI applications for the social and economic development has been growing, with a special emphasis on their financial, production, service, medical, legal, scientific, and many other applications [11: 14]. AI systems bring numerous benefits that are primarily reflected in the automation of repetitive tasks, the data generation based on machine learning algorithms, the rapid processing of huge amounts of data, the creation of significant insights and conclusions, as well as the predictions of future outcomes based on collected and evaluated data. AI drives the automation and optimization of broad business processes, and above all the company business functions and tasks, representing in this way exceptional support for the work and development of human resources, the growth of business efficiency, as well as the reduction of the risk of human error [16].

A 2023 Deloitte & Touch survey conducted in Switzerland indicates that almost 61% of respondents who work on a computer already use some of the AI programs in their daily business, while in their private life this rate is slightly higher at 64%. This research also indicates that AI systems are already widely used in the workplace, as well as that employees are very satisfied with their use, which helps them to be more productive (63%), more creative (54%) or to improve the quality of their work (45%). However, the survey results also suggest that the use of AI technology is still not systematically regulated by modern organizations and legislators [20]. Another 2024 study by the same consulting firm shows that generic AI systems are changing the way we interact, communicate and do business, making our personal and professional lives easier. From monitoring production pro-

cesses in real time to generating digital content, AI systems have reshaped the modern corporate image, bringing a number of advantages to employees and companies, as well as business success. The application of modern AI systems saves employees' time, reduces the volume of their manual work and rationalizes business processes, increasing their productivity, while enabling companies to reduce operating costs, followed by more rational use of resources and increase profitability [3].

According to McKinsey & Company global research, the use of AI technology at work almost doubled in the period between 2017 and 2022, primarily due to its ability to adapt to the unique business needs of an organization. At the same time, 63% of respondents expected further growth of their investments in AI systems in the coming period. However, modern AI systems began to be used more intensively only from 2024, when companies began to use them more comprehensevly, also by creating and generating business value for themselves. The results of this global survey also suggest that 65% of respondents regularly used AI technology, while about 75% of them expected that these systems will initiate disruptive changes in many industrial and service branches. However, the research also points to numerous risks that the use of AI technology brings, primarily the risk of inaccuracy, the violation of data privacy and intellectual property rights (IP), as well as the risk of insecurity and improper use of data [17]. In addition, although AI market is expected to add an incredible 15.7 trillion USD to the global economy by 2030, its application still drives numerous problems and challenges that require a responsible and well-thought-out approach to creative problem solving. Along with the progress of modern AI systems, more and more complex questions will appear in the technological, ethical and social aspects of their application [10]. The goal of this article is to point out exactly these problems, as well as to shed light on the challenges, extent and scope of the current use of AI technologies in the Republic of Serbia (RS).

Problems and challenges of using AI technologies in business operations

Many authors vividly state various challenges, obstacles and problems in using modern AI technologies in the contemporary workplace (Table 1). Their application brings numerous ethical, moral and regulatory considerations that mainly relate to data security and privacy, transparency, reliability of AI results and bias of their use. Along with the development of AI systems, there is also a justified concern regarding their use in a socially responsible and fair manner, as well as the possible disruption and disappearance of certain jobs and workplaces within which the AI driven automation of business processes has the possibility to completely change the contemporary labour market landscape, by creating new jobs for which it will be necessary to retrain employees and shape a new set of skills. Finally, since AI technology systems are based on the processing of huge amounts of sensitive private data, it is crucial to maintain trust in these technologies, with the appropriate use and suitable methods of protecting private data. Soni et al. [18: 2207] state that a special problem with AI technologies reflects in their unequal regional dispersion, as well as in the emergence of a kind of AI divide on a global scale that strengthens social, economic and cultural inequalities. In addition to the vulnerability and malfunction of AI software and the unreliability of AI outcomes, the challenges of using AI technologies also include a lack of trust, ethical concerns, biases, and a lack of AI talents.

Horák and Turková [7: 2 – 3] also assert that the most important sources of concerns related to the application of AI technologies include abuses in breaching protection, loss of jobs and replacement of human work by robots, although the development of AI systems does not necessarily always have a negative impact on human jobs since there are still significant differences among jobs performed by humans and jobs based on AI. Bartneck et al. [2], in

their extensive book, emphasize that the risks of using modern AI systems and in general advanced technology arise from the lack or loss of control over AI-based business operations, regardless of whether it is about the management of autonomous vehicles (AVs), electrical networks or other infrastructural facilities. In addition to this type of risk, the authors highlight the presence of numerous ethical concerns, which are reflected in the danger of corruption, discrimination, systemic abuse of human rights and their psychological impact on individuals. In addition to the unequivocal benefits and positive impacts of AI on overall business operations, Painoli et al. [14: 1384 – 1385] also point to numerous challenges and obstacles that modern companies face when relying on AI technologies. They may cause the fear of endangering the ultimate role of humans in business operations, provoking long-standing debates about the future of modern society if robots become smarter than humans. Table 1 provides a detailed overview of all risks identified by the analysed authors in this field.

Table 1. **Problems and obstacles in the use of AI technology in modern business practice**

Author(s) and year of publication	**Identified challenges and problems**
Soni et al. (2020)	Unequal regional distribution and global AI divide (divide) Vulnerability, unreliability and malfunction of AI software Lack of trust, ethical issues and bias High expectations and lack of knowledge about AI Lack of AI talents
Bartneck et al. (2021)	Absence and loss of control over AI-based business functions Ethical risks such as the risk of corruption, discrimination, systemic abuse of human rights and psychological impact on individuals Risk of system malfunction Systemic risk and fraud risk Security risk and legal risk Business reputation risk and social risk Risk of environmental disasters
Painoli et al. (2021)	Fear of compromising the role of humans in business operations Data collection, storage and required infrastructure Reluctance to invest in expensive AI technologies The degree of integration of AI into existing infrastructure and business processes Violation of consumer confidence Legal challenges Dependence on complex algorithms Impact on the work morale of employees
Gupta et al. (2023)	Numerous ethical and regulatory considerations Bias and (in)reliability of AI solutions Disruption of business Data security and privacy Lack of openness and transparency
Horák and Turková (2023)	Abuses in breaching protection Loss of jobs Replacing human work with robots

Source: *Authors' analysis.*

Application of AI technology in the Republic of Serbia

On January 10, 2025, the Government of the Republic of Serbia (RS) adopted a new Strategy for the Development of Artificial Intelligence for the period from 2025 to 2030, which emphasizes the need for further accelerated development of AI on the territory of the country. It is an umbrella document and the starting point for other legislative and action planning documents in the field of artificial intelligence, which highlights the further development of scientific research, innovation, education, economic growth and improving the quality of citizens' life. Official sources state that Serbia made an important step forward in managing the AI development and positioned itself as a leader in the Southeast European (SEE) region, which was recognized through its presidency of the Global Partnership for Artificial Intelligence, as well as its membership in the Association for Artificial Intelligence Management of the World Economic Forum (WEF) from Davos. Current projections show that the value of the global AI market amounts to more than 184 billion USD, and that by the end of 2030 this market will reach the value of 826 billion USD. On the other hand, according to the report of the European Commission (EC), it is expected that AI will significantly contribute to the automation of 14% of existing jobs, while another 32% of occupations will experience large and deep transformational changes.

Therefore, the new Strategy insists on further development in the areas of the legislative framework, investments in education, innovation and infrastructure, as well as on the increased application of AI in the public sector, tracing the path towards the modernization of the state and society as a whole. The Strategy envisages additional investments in computer infrastructure and the National Platform for Artificial Intelligence, as well as generally greater support for the application of modern AI technologies. More precisely, the RS Government plans to invest 30 million euros in an additional supercomputer, 20 million euros in software for the public sector functioning, primarily for the development of healthcare, energy and transport, and finally additional 30 million euros in incentives for the development of AI [12].

Thus, Serbia plans to invest up to 100 million euros in the development of AI by 2026 in its intention to rank itself among the leaders of the SEE region in this area. While the issue of AI related legislative activity was initiated in 2023, along with the adoption of Ethical Guidelines for the AI development and use, the focus of the new Strategy is to ensure more flexible regulation and provide reliefs to innovative companies. The emphasis is also on investments in start-up companies, since a quarter of them are already actively developing their AI solutions. The focus will also be on the further development of broadband Internet, as well as on the permanent improvements of digital infrastructure and 5G technology, the concept of smart cities, the creation of an knowledge based economy and the development of systems for data reuse and protection through the expansion of Ai solutions [13]. According to the AI Preparedness Index (AIPI) for 2024, which assesses the level of preparedness of 174 considered countries for the AI use, based on perceived indicators of a) digital infrastructure, b) available human resources and labour market policy, c) innovation and AI economic integration, and d) regulation and ethics [9], Serbia, as a leader in the Western Balkans region, ranks 52nd (score 0.54). The country is followed in this respect by Albania (59th place, score 0.53), Montenegro (65th rank, score 0.50), North Macedonia (77th place, score 0.48) and Bosnia and Herzegovina (97th rank, score 0.43) [5].

Application of AI technology in the national business sector

However, despite all these efforts, the application of AI solutions in the business of Serbian companies is still in its infancy. Non-familiarity with this technology, insufficient

degree of digitalization, high implementation costs, as well as lack of AI professional staff are among the main obstacles to a greater AI software application. Although the RS Government has a proactive attitude towards the adoption of AI at the national level, it is estimated that in Serbia still a small number of companies use this technology in their business, while the development of AI takes place very quickly, so it is logical that the pace of its implementation is slower. In addition, Serbia faces numerous challenges on this front. A qualified workforce with specific AI skills is still insufficient and limited. The education system and the labour market do not produce a sufficient number of experts in this field, which slows down the process of its adoption. For small and medium-sized companies, the introduction of AI also requires significant resources, which include the procurement of the necessary equipment, software development, but also investment in employee education. At the same time, many companies do not have the opportunity to invest in these technologies without support or subsidies from the state. In addition, for the introduction of AI systems, prior consolidation of data, as well as their transfer to modern platforms where they can be processed still requires significant financial resources and time.

However, Serbia recognized the fact that AI is not something that is „nice to have", but that it represents a key value that differentiates companies from their competition. In these processes, it will be particularly challenging to develop national regulation in the field of AI, with the need to rely on the European Law on Artificial Intelligence, which tends to establish a balance between unrestrainable technological innovations and the protection of basic rights and privacy of citizens. A special focus should be on data security and civil rights protection, while at the same time further integration of AI, investment in new technologies and application of innovation should be enabled. Regulation should be developed that sanctions all AI uses with dominantly unfavourable aspects. Finally, there is a need for education, training, specialisation and retraining of IT personnel in programming, artificial intelligence, cyber security and other relevant areas, so that their supply could be aligned with the needs of the national labour market demand [19].

Despite this, in the last few years, Serbia has grown into a significant centre for the development of AI technologies in the Western Balkans. This growth is fuelled by a variety of factors, including the availability of young AI talents, a strong IT industry and increased interest in technologies that can transform contemporary business models and improve efficiency. Recent research on a sample of 157 Serbian companies of various sizes and industries indicates that only one third (34%) of the surveyed companies has some experience in the AI application. The largest application of AI was recorded in the information, communication and professional sectors, where even 60% of companies use these technologies. On the other hand, traditional industries, such as processing industry, lag behind in digitization and automation, although they have enormous potential for optimizing business processes. However, there are also the biggest challenges in this industry, considering the complexity of these systems and problems that may arise when integrating AI systems into the existing business structure.

At the same time, only large companies in Serbia appear as leaders in the application of AI technologies, while 85% of them have a formalized strategic approach to its development. In medium-sized companies, that percentage is slightly lower and amounts to 74%, while only 27.9% of small companies have developed strategies for applying AI in their business processes, which indicates limited resources and a lack of expertise in smaller organizations. Most of them cite increased efficiency, improved quality of products and services, and reduced operating costs as benefits of AI technologies. However, these companies also face numerous obstacles and challenges, dominated by poor data quality, a lack of experts in areas such as machine learning and data analytics, and difficulties in integrating AI solutions with existing systems such as enterprise resource planning (ERP) and customer

relationship management (CRM) platforms. Simultaneously, more than 65% of smaller companies in Serbia still do not use AI systems, mainly because they are not relevant to their industry, due to lack of knowledge and skills, or due to high implementation costs [8]. At the same instant, large companies with a developed strategic approach to innovation play a dominant role in the national AI landscape. The strategic approach to AI is most prevalent in the sectors of communications and information, but also in professional, scientific, innovation and technical activities. Apart from them, the application of AI technology is somewhat more pronounced in the financial and insurance activities and real estate business. Products that are based on AI or on the use of AI technologies have been launched by less than a fifth of domestic companies, while more complex products that would cover more business functions and areas still represent exceptions among Serbian companies [1].

Concluding remarks

In Serbia, the application of AI technologies in the company business is still in its infancy. The Serbian economy has great potential for the growth of the use of AI systems, especially in traditional industries that, with adequate support, could experience a significant transformation. Education, automation of business processes and strategic investments are recognized as key factors for the spread of AI technologies in various economic branches. Companies that do not use them cite implementation costs, lack of knowledge and the perception that AI is not relevant to their industry as the main reasons for not adopting it. At the same time, education and development of human capital are also recognized as the most important steps in spreading the application of AI technologies in Serbia. Many companies plan to invest in automation and business analytics in the near future, while more complex projects are expected in the coming years. The key for further progressing lies in a strategic approach to development, improving the quality of data and strengthening cooperation among the private sector, start-up companies and public institutions [8]. However, if we were to look at the fundamental obstacles in the use of modern AI technologies from Table 1, we could conclude that there are numerous challenges in Serbia that are primarily reflected in data security and privacy, lack of trust and AI talents, high implementation costs, ethical issues, lack of knowledge about AI technologies, (un)reliability of AI solutions, as well as in the risk of fraud and security risk.

The use of AI technologies is still relatively low in Serbian companies, mainly spreading in the business practice of large and medium-sized companies and in ICT and professional, scientific, innovative and technical activities. This is not surprising considering that the use of AI technologies in these companies is a prerequisite for their survival on the global market, while such organizations are also characterized by huge developmental opportunities. The experiences of national companies indicate that for achieving success in the AI application and development, both in an operational and strategic sense, it is necessary to develop an adequate business strategy, to have an active attitude towards talent recruitment and to apply it widely within the companies, while it is also necessary to establish and nurture multiple relations in the innovation and IT ecosystem, with the irreplaceable role of external experts and experienced technology companies. At the same time, there is a very low degree of AI application in traditional industries, which is the domain with the greatest development potential and opportunities for influencing the wider economic, innovative and social development of the country.

In Serbia, legal solutions that insist on data security and the protection of data privacy should be further developed, by requiring thorough testing procedures, careful management of data quality documentation and identifying supervision liabilities. There is also a need for classifying contemporary AI systems into high, limited and low risk categories in

order to precisely regulate the conditions of their using, as well as to ensure the integrity and protection of the AI users. In 2018, the RS Government also adopted a new Personal Data Protection Act that changed the way companies collect and process personal data. Relatedly, companies have increasingly placed an emphasis on investments in security in order to reduce the risk of surveillance, hacking and cyber-attacks. The issues of data protection and the use of AI should be considered together since this aspect often involves the collection, processing and analysing of large amounts of data. The application of AI in business implies that these operations should adhere to the principles of legality, fairness and transparency, which should include the full providing of comprehensive and transparent information to individuals whose personal data is processed, as well as the way of their collection and handling [15]. Finally, domestic companies should have to conduct detailed risk assessments of their AI systems to ensure their compliance with generally accepted moral principles, ethical standards and applicable security regulations.

References

1. **Andrejić,** M. (2025). AI tehnologije u Srbiji koriste uglavnom velika i srednja preduzeća, najveći potencijal u tradicionalnoj industriji (AI technologies in Serbia are used mainly by large and medium-sized companies, the biggest potential in traditional industry). – In: *Biznis.rs*, February 1, 2025. [available 22.02.2025]. *https://biznis.rs/novac/investicije/ai-tehnologije-u-srbiji-koriste-uglavnom-velika-i-srednja-preduzeca-najveci-potencijal-u-tradicionalnoj-industriji/.*
2. **Bartneck,** C., C. Lütge, A. Wagner & S. Welsh. (2021). Risks in the Business of AI. Chapter 6. – In: *An* Introduction to Ethics in Robotics and AI. Springer, 2021.
3. **Beierschoder,** M. (2024). Artificial Intelligence Is Changing How Companies Work. – In: *Deloitte*, May 30, 2024. [available 21.02.2025]. *https://www.deloitte.com/ch/en/Industries/technology/perspectives/artificial-intelligence-Is-changing-how-companies-work.html*.
4. **Bell,** E. (2025). How AI Is Used in Business. – In: *Investopedia*, January 29, 2025. [available 20.02.2025]. *https://www.investopedia.com/how-ai-is-used-in-business-8611256*.
5. **Digital** Information World. (2025). Which Nations Excel and Struggle in the IMF's AI Preparedness Index? June 11, 2024. [online]. [available 22.02.2025]. *https://www.digitalinformationworld.com/2024/11/which-nations-excel-and-struggle-in.html*.
6. **Gupta,** R., H. Katoch & C. Philosophers. (2023). Role of Artificial Intelligence in Business Management. – In: *International* Journal for Multidimensional Research Persspective, 1(3), p.p. 175-184.
7. **Horák**, J. & M. Turková. (2023). Using artificial intelligence as business opportunities on the market: An overview. – In: *SHS* Web of Conferences, 160(01012), p.p. 1-12. [online]. *https://doi.org/10.1051/shsconf/202316001012.*
8. **ICT** Hub Empowering Innovation. (2025). Veštačka inteligencija u Srbiji: Samo trećina kompanija koristi AI – šta ih koči? (Artificial intelligence in Serbia: Only a third of companies use AI – what's holding them back?). – In: *ICT* Hub. [online]. [available 22.02.2025]. *https://www.icthub.rs/clanak/vestacka-inteligencija-u-srbiji-samo-trecina-kompanija-koristi-ai-sta-ih-koci*.
9. **International** Monetary Fund. (2025). AI Preparedness Index (AIPI). [online]. [available 22.02.2025]. *https://www.imf.org/external/datamapper/datasets/AIPI#:~:text=AI%20Preparedness%20Index%20(AIPI)%20assesses,integration%2C%20and%20regulation%20and%20ethics.*
10. **Kumar,** A. (2025). Top 15 Challenges of Artificial Intelligence in 2025. – In: *SimpliLearn*, February 17, 2025. [online]. [available 21.02.2025]. *https://www.simplilearn.com/challenges-of-artificial-intelligence-article*.
11. **Madžar,** L. & M. Simić. (2025). Education, knowledge and key human-centric skills in the era of artificial intelligence. – In: *Znanje* ili veštine vs. Znanje i veštine. Belgrad: Institut za strategijske studije i razvoj „Petar Karić“ & Naučno društvo za upravljanje organizacijama, p.p. 13-26. DOI: 10.46793/Znanje25.13M.
12. **Ministarstvo** nauke, tehnološkog razvoja i inovacija. (2025). Usvojena Strategija za razvoj veštačke inteligencije u Republici Srbiji za period od 2025. do 2030. godine (Adopted Strategy for the Artificial Intelligence Development in the Republic of Serbia for the period from 2025 to 2030).

January 10, 2025. [online]. [available 21.02.2025]. *https://nitra.gov.rs/cir/ministarstvo/vesti/usvojena-strategija-za-razvoj-vestacke-inteligencije-u-republici-srbiji-za-period-od-2025-do-2030-godine*.

13. **Naled.** (2024). Srbija u razvoj veštačke inteligencije ulaže 100 miliona evra do 2026 (Serbia is investing 100 million euros in the development of artificial intelligence until 2026). – In: *Naled*, February 22, 2024. [online]. [available 22.02.2025]. *https://naled.rs/vest-srbija-u-razvoj-vestacke-inteligencije-ulaze-100-miliona-evra-do-2026-8731*.
14. **Painoli,** G. K., R. Madhusudan, V. Datrika, N. Chowdary & N. Kalgi. (2021). Artificial Intelligence In Business – Benefits And Challenges. – In: *Turkish* Online Journal of Qualitative Inquiry (TOJQI), 12(5), p.p. 1377-1388.
15. **Pekić,** S. (2024). Pravna regulativa veštačke inteligencije (AI) (Legal regulation of artificial intelligence (AI). [online]. [available 22.02.2025]. *https://attorney.rs/pravna-regulativa-vestacke-inteligencije-ai/*.
16. **Quiroz-Vázquez,** C. & M. Goodwin. (2024). What is artificial intelligence (AI) in business? – In: *IBM*, February 20, 2024. [online]. [available 20.02.2025]. *https://www.ibm.com/think/topics/artificial-intelligence-business*.
17. **Singla,** A., A. Sukharevsky, L. Yee, M. Chui & Bryce Hall. (2024). The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. – In: *McKinsey*, May 30, 2024. [online]. [available 21.02.2025]. *https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai*.
18. **Soni,** N., E. K. Sharma, N. Singh & A. Kapoor. (2020). Artificial Intelligence in Business: From Research and Innovation to Market Deployment. – In: *International* Conference on Computational Intelligence and Data Science (ICCIDS 2019), Procedia Computer Science, 167 (2020), p.p. 2200-2210.
19. **Tanjug.** (2024). Primena veštačke inteligencije u poslovanju kompanija u Srbiji (Application of artificial intelligence in the business operations of companies in Serbia). – In: *NewsMax* Balkans, October 25, 2024. [online]. [available 22.02.2025]. *https://newsmaxbalkans.com/ekonomija/vesti/2775/primena-vestacke-inteligencije-u-srbiji/vest*.
20. **Wiget,** M. & K. Capellini. (2023). AI study: Over 60 per cent use Artificial Intelligence at work – almost half of all employees are worried about losing their jobs. – In: *Deloitte*, August 28, 2023. [online]. [available 21.02.2025]. *https://www.deloitte.com/ch/en/about/press-room/ai-study-almost-half-of-all-employees-are-worried-about-losing-their-jobs.html*.

THE NECESSITY OF DECISIVE COUNTERINTELLIGENCE PROTECTION AND SUPPRESSION OF VITAL STATE VALUES FROM ORGANIZED CRIME

Assoc. Prof. Aleksandra Jovanovic, PhD
Faculty of Business Economics and Entrepreneurship – Belgrade, Serbia

НЕОБХОДИМОСТТА ОТ РЕШИТЕЛНА КОНТРАРАЗУЗНАВАТЕЛНА ЗАЩИТА И ПОТИСКАНЕ НА ЖИЗНЕНОВАЖНИ ДЪРЖАВНИ ЦЕННОСТИ ОТ ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ

доц. д-р Александра Йованович
Факултет по бизнес икономика и предприемачество – Белград, Сърбия

Abstract: *All states, regardless of the system of political power, possess identified crucial vital state values, which they decisively defend by ensuring stable and predictable national security. In order to ensure its own survival and sustainable development, the state establishes a system of national security by protecting its vital values, as set out in the Constitution. The article presents the necessity of decisive counterintelligence protection of vital state values from organized crime, which is achieved through the application of numerous methods and means, relying on state and social entities.*

Key words: *counterintelligence; vital state assets; organized crime; intelligence; national security; cyberspace*

Резюме: *Всички държави независимо от системата на политическа власт притежават идентифицирани жизненоважни държавни ценности, които решително защитават, осигурявайки стабилна и предвидима национална сигурност. За да осигури собственото си оцеляване и устойчиво развитие, държавата създава система за национална сигурност, като защитава нейните жизнени ценности, заложени в Конституцията. Докладът показва необходимостта от съдебна контраразузнавателна защита на жизненоважни държавни ценности от организираната престъпност, което се постига чрез прилагане на множество методи и средства, разчитащи на държавни и обществени субекти.*

Ключови думи: *контраразузнавателна дейност; жизненоважни държавни ценности; организирана престъпност; разузнаване; национална сигурност; киберпространство*

Introduction

The distrust between states reflects the ongoing conflict between secret intelligence and counterintelligence activities between many states. Each state seeks to uncompromisingly protect vital state and social values and other interests. The state as a community, which synthesizes activities, strives to realize the interests of its citizens (territorial integrity, sovereignty, social order, i.e. state power, rights, freedoms and obligations of citizens) – the protection of vital or national interests. Achieving this goal presupposes the ability of the state, through the coordinated rational use of its capacities (its power), to produce changes within its borders and in its environment that reflect the state of optimal protection of its own vital values from threatening activities (Lakićević 2022, p.p. 123-145). In order to achieve this goal, the state must establish certain mechanisms or systems to protect its own secrets from external and internal intelligence agents, or to protect itself from internal and external dangers. In order to eliminate threats and preserve the security of the state and its constitutional category, the state must have an organized system that performs its tasks

through the security and intelligence function (Mijalkovski 2009, p. 162). The central categories of the intelligence phenomenon are intelligence activity, intelligence service and security information system (Mijalković 2010), and counterintelligence activities.

In order to effectively protect its vital assets from intelligence aggression, the state regulates a complex of security measures based on counterintelligence measures. To achieve this goal, the state obliges counterintelligence or security services whose task is to engage in activities for the purpose of national security. The effectiveness of a state's counterintelligence activities is significant, especially in terms of suppressing the most dangerous types of threatening activities such as organized crime and illegal activities in cyberspace. The priority interests of every state should be focused on preserving territorial integrity, the inviolability of borders, and the protection of citizens and material goods. In the last fifteen years, the question has been raised as to whether and to what extent the interests of the Republic of Serbia in terms of territorial integrity and material assets have been protected from internal and external threats.

. The construction of a human community becomes a logical consequence of intelligence, which a person acquires through a continuous process of cognition, as a consequence of human curiosity (Lončar & Marić 2022, p.p. 107-126). This is the reason for the importance of considering the place, role and influence of intelligence and counterintelligence as significant segments of the protection of the vital interests of society and deserving of being the subject of special interest and research.

Objective and methods

The scientific goal of the article is a scientific description and explanation of counterintelligence protection of vital national values of the state from intelligence activities for the purposes of organized crime.

The practical goal of the article is to provide scientific knowledge that will contribute to a more efficient suppression of intelligence agents and the improvement of the system of counterintelligence protection of the vital national values of the state. The scientific and social justification of the article lies in its scientific and practical goal.

The methods applied in the article are: content analysis, abstraction method, legal-dogmatic method.

Defining counterintelligence protection

„Counterintelligence protection“ of the vital values of the state implies protection (of someone or something) from someone's intelligence activities (attacks), protection from the intelligence activities of external (primarily from the state) and internal (organized criminal and terrorist groups) entities (Stajić 2005, p. 214). According to Webster's dictionary, counterintelligence activity is an organized activity of intelligence services, aimed at preventing the actions of enemy information potentials, deceiving the enemy, preventing sabotage, and collecting political and military information. As already stated, counterintelligence activity is, first and foremost, an activity aimed at understanding and neutralizing all aspects of intelligence activity – intelligence operations of enemy entities (Bajagić 2009, p. 374).

In the suppression of external activities in the form of espionage and subversive activities, and thus the suppression of organized crime and terrorism, in the suppression of external espionage and subversive activities on the territory of the Republic of Serbia, all secret services participate as a special intelligence and security system (National Security Strategy 2019, p. 30). To this end, this system undertakes numerous and diverse counterintelligence activities.

The purpose of counterintelligence activities is to optimally contribute to the adequate assessment of the goals and capabilities of those carrying out threatening activities (Lakićević 2022, p. 123). Considering the purpose of the state's counterintelligence activity – „dismantling the cover-up of organized crime“, it is clear that this activity represents the most deadly weapon for suppressing the intelligence activities of organized crime leaders Counterintelligence is a planned, organized, secret and continuous offensive-defensive operational engagement of the security services of a certain state, primarily on its territory, for the purpose of detecting, monitoring, intercepting and disabling the activities of foreign intelligence services, individual persons, groups and organizations on the territory of one's own state directed against national security (Đorđević 1986, p. 183).

The task of counterintelligence is to protect state and other types of secrets from external intelligence agents. In order to effectively fulfill this task, it is necessary to develop it in terms of technical and technological modernization of work and the adoption of new methods of action, as well as to conduct increasingly frequent offensive activities in order to maintain the reliability and efficiency of the protection of the national security system. Today, states are adopting new national security strategies, counterintelligence and counterterrorism strategies, and are thus taking certain steps towards reorganizing the national security system.

Intelligence operators, intelligence services and agencies undertake activities with the aim of collecting data, which they rank in multiple stages by applying methods using human resources and technical means. The collected data is analyzed and evaluated and delivered to the parent entity, which uses it when making decisions on the protection of national interests and vital state values.

The performance of counterintelligence operations was accompanied by respect for the basic principles of work: alignment with the mission, secrecy of work (avoiding publicity), objectivity, confirmation of the reliability of the collected data, offensiveness, flexibility (adaptability), continuity, and continuity (Counterintelligence Operations 1993, p. 24). It is precisely this secrecy that makes it impossible to explain and provide examples of counterintelligence activities more precisely.

Intelligence and counterintelligence constitute a complex process, which consists of the following stages: 1) determination of intelligence (information) needs; 2) transmission of intelligence requests to intelligence services; 3) initiative phase.

One of the basic functions of counterintelligence is the collection of information about foreign intelligence services and their activities and intentions, from which the basic conspiratorial methods of data collection can be determined, including: the agent (classical) method; the method of infiltration into enemy structures; the method of secret use of technical means and the method of covert data collection. A method of covert data collection that is implemented through: 1) covert observation; 2) covert surveying; and 3) covert scientific research. The agent method, the basic method for gathering knowledge about an adversary's secrets, is based on a secretly established (non-professional) relationship between an individual and the intelligence/counterintelligence service that initiated such a relationship. The infiltration method is characteristic of both (offensive) counterintelligence and intelligence services, or activities.

Counterintelligence activities in the function of combating organized crime

Proactive action in combating crime means criminal activity that is undertaken spatially and temporally in the criminal precinct (Harfield 2000, p. 109). Here, the basis of action is the effort to be „present on the ground“ and well informed about all conditions and problems that exist in the given environment, which favor or lead to the commission of

criminal acts. This means that the basis of proactive action is not a specifically committed criminal act, but special methods are applied in this case. A proactive approach involves anticipating potential manifestations of anti-social and anti-social behavior and acting in advance, with the aim of preventing criminal acts, unlike the reaction to crime which is undertaken post festum and is nothing more than a belated social response to crime (Marinković 2006, p. 26).

A special counterintelligence method occurs in the event of the commission or warning of the commission of a criminal offense. After the first phase of counterintelligence activities – confirming the indication that a criminal offense has been committed by a specific person, the second phase follows – with the approval of the court, special evidentiary actions are carried out until the filing of criminal charges (Jovanović 2024, p.p. 166-212). In this phase, the special public prosecutor, in cooperation with the person responsible for the counterintelligence-operational evidentiary procedure, conducts investigative actions. Based on the evidence gathered, an indictment is issued. The third phase – the phase of the criminal procedure is conducted by the Special Department of the Higher Court in Belgrade for Organized Crime. The third phase ends with the issuance of a first-instance verdict. The possible fourth phase represents the confiscation of property gains acquired through the criminal offense of organized crime. In addition to the fact that Serbia has built a system of institutions that have the authority to combat organized crime, the reform of the fight against it normatively regulates special investigative methods and techniques for confiscating property resulting from a criminal offense (Banović 2016, p. 177).

Given that the basic method of operation of organized criminal groups is clandestine action through investing illegally acquired money in legal flows and providing money or material goods to corrupt employees in the state administration, in order to achieve the goal of these groups: the possibility of financing illegal actions and reporting important information, it is necessary to decode such illegal actions through counterintelligence activities and thereby achieve the protection of the vital assets of the state. This action prevents organized criminal groups from transforming property profits into a political goal. Sources of information on the risk of organized crime are: human sources (undercover investigator and witness collaborator), controlled delivery, information obtained based on covert source methods (wiretapping of mobile phones; wiretapping of communications of certain persons; surveillance of persons, objects and spaces).

The current normative and institutional environment dictates the necessity of a multi-agency approach to combating organized crime, both on a preventive and repressive level. On the other hand, the issue of duplication of competences and the adequacy of the capacities of certain bodies authorized to combat organized crime is raised. Thus, for example, it is considered „that it is necessary to establish the jurisdiction of the police for the implementation of certain special investigative measures independently of the security-intelligence services in accordance with EU standards“.

In the Republic of Serbia, the bodies established by law, under the authority and control of the government as the bearers of the fight against organized crime are: the Service for Combating Organized Crime (SBPOK) of the Ministry of Internal Affairs, the Security and Information Agency, The Military Security Agency as an administrative body within the Ministry of Defense, the Special Court Departments and the Special Prosecutor's Department for Organized Crime of the Ministry of Justice, the Anti-Money Laundering Administration, the Tax Administration and the Customs Administration of the Ministry of Finance. In order to resolve individual issues, the government may form temporary working bodies whose work is directed and supervised by the National Security Council. The work of these bodies must be coordinated with the criminal intelligence activities of the competent services. The aforementioned bodies conduct counterintelligence assessments and plan

measures to protect vital assets from organized criminal activity, which are confirmed by the competent head of the primary service. Intelligence services provide data that enable the executive branch to identify threats to the vital values of society and the state, by collecting, analyzing, and storing data on threats aimed at national security, and by preparing policies for their protection (Đurđević & Stevanović 2016, p. 2). In addition to the primary recognition of activities and the bearer of activities aimed at the vital values of the state, these services also perform related counterintelligence tasks, such as recognition and opposition to the secret and organized activities of foreign intelligence services and groups, and often security protection of information and information systems of the state (Mijalković 2011, p.p. 74-92). In the security system of some countries, subjects of the international security sector, both civil and military, both intergovernmental and non-governmental, are noticeable (Mijalković 2010, p. 253).

It can be said that all sectors or services work towards examining the level of threats or threats to the vital values of society. Unfortunately, determining the precise value of the security threat is not possible because organized crime entities conceal their income from authorities through illegal actions (Korac 2011, p. 446), and these threats can only be assessed partially, based on judicial and police statistics. To complement this assessment, the effects of transnational organized crime on the performance of vital public functions are considered: the protection of human rights and social well-being, respect for the rule of law, democratic access to the work of institutions, the preservation of cultural heritage, etc. In recent months, the question of the existence of internal organized crime and its impact on the aforementioned vital functions has been raised in Serbia. The initiative to resolve this issue is not seen within the executive branch and intelligence services, which does not mean that intelligence services and counterintelligence are inactive.

The services start from suspicions of the existence of organized criminal activity, which is the basis for the application of counterintelligence measures. The starting point for establishing suspicion is a search of internal databases with a focus on general indicative facts. These indications are based on national and international experiences. We will highlight some of the indications: people who do not have legal income live on a „high foot"; murders occur; explosives are planted under vehicles, in shops and apartments; fires are set without clear motives; murders are committed with weapons that are not available to citizens; there are no witnesses, although the murders were committed in a public place in the presence of citizens; the injured parties and victims refuse to cooperate with the police and to testify in court, etc. (Simonović 2004, p. 631). In order to recognize, confirm and clarify indications (whistleblowers) about the emergence of organized crime, primary informants apply general counterintelligence methods and secondary operational methods (informative interviews, analysis of criminal charges, analysis of certain documentation, analysis of public transport and spot checks of public transport for the purpose of identifying persons, inspecting goods, etc.). In addition to the general method, special methods are also applied, which criminal theory defines as evidentiary actions against a person for whom there are grounds for suspicion that he or she has committed a criminal act of organized crime, and where evidence for criminal prosecution cannot be collected in any other way or its collection would be difficult. Unlike special methods that are not approved by the court, evidentiary actions are carried out with the approval of the court and in accordance with the provisions of the Criminal Procedure Code. The court controls the implementation of the legality of these actions, which represent covert infiltration and covert surveillance methods. The development of science and technology provided great opportunities for the expansion of the application of secret methods of investigating criminal offenses, and directed criminal proceedings towards the area of secret – discreet monitoring and exposure of complex processes and structures of organized crime (Marinković 2006, p. 29).

Counterintelligence activities in cyberspace

Counterintelligence activities today also include protection in cyberspace, in places that are security-sensitive and rely on information systems. Its functions are: detection, identification, assessment, neutralization or exploitation. Particular attention should be paid to the protection of critical infrastructure, which consists of strategy, policy, and preparedness to prevent or respond to an attack. Controlling cyberspace is difficult because intelligence and counterintelligence services were once unable to monitor communications, except when monitoring traffic between precisely designated email addresses. Terrorists are increasingly using the possibilities of cyberspace, and the activities of services in this field are significant. Terrorists are increasingly using cyberspace for communication, so intelligence and due to the complexity and importance of actions against terrorist attacks, continuous international cooperation, exchange of data and expert experiences are necessary (Jovanović 2019, p.p. 205-2018). This enables the development of better systems for protection and prevention of terrorist attacks.

Defining threats that endanger information structures is made difficult by the complexity of cyberspace and the large number of potential attackers in cyberspace (individuals with criminal intentions, individual criminals, organized criminals, organized crime, terrorists, extremist groups, and even states whose motives are diverse: influence, theft, espionage, warfare). The number and diversity of potential attackers and potential threats leads to the need to form specialized bodies and programs in the services dealing with intelligence and counterintelligence.

The activities of intelligence services in cyberspace in the form of internet trolling enable covert access to primary data on the territory of other states, which allows intelligence officers to directly carry out their intelligence/counterintelligence tasks on the territory of other states (Shorer-Zeltser, Ben-Israel 2016, p.p. 102-122). Thus, this method is offensive in nature, but it is also necessary to respect intelligence ethics, which implies respect for the social code of conduct. Operating in another country's cyberspace instead of cooperating with institutions raises questions of legitimacy. This method is resorted to even when it comes to the common interests of states in the fight against organized crime and terrorism. On the other hand, from the aspect of protecting national security in cyberspace, the risk is also posed by the fact that this method often represents an effort by intelligence services and counterintelligence to change public opinion.

Conclusion

The scientific and professional community and political entities, both nationally and internationally, have a unified view that organized crime is one of the most dangerous security threats today, a threat to the vital interests of society. Although there is community consensus on what constitutes the greatest threat to the vital interests of society, there is no unified identification and conceptual determination of the dimensions and choice of methods for combating organized crime. The challenge posed by organized crime requires a strong, skilled and adequate response. Such a response depends on the timely information necessary to determine the conditions and time needed for an optimal response to organized crime. The vital values of the state, a constant subject of interest of intelligence services of other states and non-state entities, are monitored by planning, organizing and undertaking intelligence activities using covert and public methods in order to obtain sensitive data in order to use them in actions and planning to threaten vital values. The danger of this type of activity also involves the creation of a network of collaborators among domestic citizens, which leads to the necessity of multidimensional use of the agent network. Such actions by foreign

intelligence services and espionage require a response, in which counterintelligence and services organized to protect national security play a role. This is where intelligence services and counterintelligence come in to take preventive action or suppress organized crime by applying adequate methods.

Literature

1. **Bajagić,** M. (2009). Inostrana iskustva u razvoju teorijskog i organizacionog koncepta kontraobaveštajne aktivnosti. – In: *Bezbednost,* Beograd, p.p. 370-385.
2. **Banović,** B. (2016). Organizovani kriminal kao aktuelna bezbednosna pretnja. – In: *Internationals* problems, MP, Vol. LXVIII, br. 2-3, str. 172-192. DOI:10.2298/MEDJP1603172B.
3. **Counterintelligence** Operations. (1993). Headquarters Department of the Army US. – In: *Washington* DC, No. 30-17, п. 24.
4. **Đorđević,** O. (1986). Leksikon bezbednosti. – In: *Partizanska* knjiga, Beograd, p. 183.
5. **Dragišić,** Z. (2009). Sistem nacionalne bezbednosti: Pokušaj definisanja pojma. – In: *Vojno* delo, 3/2009, pp. 162-176.
6. **Đurđević,** Ž., M. Stevanović. (2016). Obrazovanje za nacionalnu bezbednost. – In: *Akademska* misao, Beograd.
7. **Đurdjević,** D., M. Stevanović. (2016). Internet trolovanje kao metod ofanzivnog obaveštajnog delovanja u kiberprostoru. – In: *Žurnal* za kriminalistiku i pravo, pp. 13-31. DOI: 10.5937/nabepo22-12060.
8. **Harfield,** C. Pro-activity, Partnership and Prevention. – In: *The* Police Journal, 2000, br. 2, str. 109.
9. **Izveštaj** o napretku Srbije za 2012. godinu. Evropska komisija, Brisel, 10.10.2012. SEC (2012)333, str. 75.
10. **Jovanović,** A. (2019). Organizing a european security strategy and cyber security in the Republic of Serbia as a response to cyber terrorism. – In: *Međunarodna* naučna konferenija „Savremeni trendovi u razvoju saobraćaja i bezbednosti regiona jugoistočne Evrope", „Konstantin Veliki", Niš, pp. 205-218.
11. **Jovanović,** A. (2024). Krivičnoprocesno parvo. Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, pp. 166-212.
12. **Korać,** S. (2011). Organizovani criminal kao bezbednosna pretnja Evropskoj uniji. – In: *Društveni* aspekti organizovanog kriminala. Beograd, pp. 410-450.
13. **Lakićević,** M. (2022). Kontraobaveštajna delatnost u funkciji suzbijanja organizovanog kriminala. – In: *Nacionalni* interes, god. XVII, vol. 41, br. 1/2022, pp. 123-145. DOI:10.22182/ni.4312022.6. [online]. *https: doi.org//10.22182/ni.4312022.6.*
14. **Lončar,** M., D. Marić. (2022). Ekonomska obaveštajnost u savremenim ekonomsko-bezbedonosnim okolnostima. – In: *Ekonomija,* teorija i praksa, god. XV, br. 2, pp. 107-126. DOI:10.5937etp2002107L.
15. **Marinković,** D. (2006). Kriminalistička strategija suzbijanja organizovanog kriminaliteta – osnovni konstitutivni elementi. – In: *Zbornik* radova: Sprečavanje i suzbijanje savremenih oblika kriminaliteta, Kriminalističko policijska akademija, pp. 13-36.
16. **Merriam** Webster dictionary. [online]. [available 20.06.2008]. *http://www.merriam-webster.com/dictionary/.*
17. **Mijalković,** S. (2010). O nedržavnom sektoru nacionalnog sistema bezbednosti – inostrana i domaća iskustva. – In: *Strani* pravni život, 2/2010, pp. 251-269.
18. **Mijalković,** S. (2010). Obaveštajne strukture terorističkih kriminalnih organizacija. – In: *Nauka,* bezbednost i policija, no 15.
19. **Mijalković,** S. (2011). Obaveštajno-bezbednosne službe i nacionalna bezbednost. – In: *Bezbednost,* br. 1, Kriminalističko-policijska akademija, Beograd, pp. 74-92.
20. **Mijalković,** S. (2010). O nedržavnom sektoru nacionalnog sistema bezbednosti – inostrana i domaća iskustva. – In: *Strani* pravni život, 2/2010, pp. 251-269.
21. **Mijalkovski,** M. (2009). Obaveštajne i bezbednosne službe. – In: *Službeni* glasnik, Beograd, pp. 32-33.
22. **Schell,** O. (2007). Follies of Orthodoxy. – In: *What* Orwell Didn't Know: Propaganda and the New Face of American Politics. A. Szántó. (Ed.). New York: Public Affairs.
23. **Shorer-Zeltser,** M., G. M. Ben-Israel. (2016). Developing Discourse and Tools for Alternative Vontent to Prevent Terror. – In: *National* Security and Counterintelligence in the Era of Cyber Espionage. E. de Silva. (Ed.). Hershey: IGI Global, pp. 102-122.
24. **Simonović,** B. (2004). Kriminalistika. Kragujevac& Pravni fakultet.
25. **Stajić,** Lj. (2005). Osnovi bezbednosti. Fakultet civilne odbrane. Beograd: Draganić.
26. **Strategija** nacionalne bezbednosti Republike Srbije. – In: *Službeni* glasnik RS, br. 94, 2019.

ДЕЙНОСТТА НА ЧУЖДИТЕ РАЗУЗНАВАНИЯ ЗА ВЗРИВЯВАНЕ НА ОФИЦИАЛНИТЕ ДИПЛОМАТИЧЕСКИ ОТНОШЕНИЯ МЕЖДУ БЪЛГАРИЯ И САЩ ПРЕЗ ПЪРВАТА СВЕТОВНА ВОЙНА

проф. д.и.н. Трендафил Митев
Висше училище по сигурност и икономика – Пловдив

THE ACTIVITIES OF FOREIGN INTELLIGENCE AGENCIES IN BLOWING UP OFFICIAL DIPLOMATIC RELATIONS BETWEEN BULGARIA AND THE UNITED STATES DURING THE FIRST WORLD WAR

Prof. Trendafil Mitev, DHS
Higher School of Security and Economics – Plovdiv

Резюме: *През годините на Първата световна война САЩ се очертават окончателно като водеща Велика сила в света. Поради това българското правителство взема правилното решение да открие Българска легация във Вашингтон. Новата инициатива се налага поради рязко активизиралата се антибългарска пропаганда на разузнавателните и пропагандните служби на Сърбия и Гърция в Америка след Междусъюзническата война. Благодарение на мъдрата политика, провеждана от първия пълномощен министър проф. Стефан Панаретов усилията на противобългарската кампания са сведени до минимум. Нещо повече, дори когато през есента на 1915 г. България е принудена да влезе в световния военен конфликт в състава на Централните сили начело с Германия, правителството на У. Уилсън запазва официалните дипломатически отношения между Вашингтон и София, защото американският политически елит е убеден, че България воюва не за заграбването на чужди територии, а за освобождението на насилствено откъснатата част от нашия народ в Македония и обединението ѝ със свободната част на Родината.*

Ключови думи: *антибългарска пропаганда; български национални интереси; съхранени дипломатически отношения; блестяща страница в отношенията между България и САЩ*

Abstract: *During the years of World War I, the United States emerged definitively as the world's leading Great Power. The Bulgarian government therefore took the right decision to open a Bulgarian Legation in Washington. The new initiative was necessitated by the sharply intensified anti-Bulgarian propaganda of the intelligence and propaganda services of Serbia and Greece in America after the Inter-Allied War. Thanks to the wise policy pursued by the first Minister Plenipotentiary Prof. Stefan Panaretov the efforts of the anti-Bulgarian campaign were minimized. Moreover, even when in the autumn of 1915. Bulgaria was forced to enter the world military conflict as part of the Central Powers led by Germany, the government of W. Wilson maintained official diplomatic relations between Washington and Sofia because the American political elite was convinced that Bulgaria was fighting not for the seizure of foreign territories but for the liberation of the forcibly separated part of our people in Macedonia and its reunification with the free part of the Motherland.*

Key words: *anti-Bulgarian propaganda; Bulgarian national interests; preserved diplomatic relations; shining page in relations between Bulgaria and the USA*

В навечерието на Първата световна война САЩ вече са най-развитата държава на планетата в икономическо отношение. Въпреки това обаче тя все още страни от основните военнополитически групировки в Стария свят – Антантата и Тройния съюз [5: 20 и сл.]. Поради това Великите сили в Европа, макар че се съобразяват с поведението на официален Вашингтон, все още третират великата северноамериканска република като „младши партньор“ в световните дела. В резултат и администрацията на

президента У. Уилсън се придържа към линия на невмешателство във вътрешноевропейските политически процеси. Защото те довеждат до избухването на Първата световна война през лятото на 1914 г. Официален Вашингтон заема неутрална позиция към разгорелия се безпрецедентен военен конфликт между Антантата (Англия, Франция и Русия) и Тройния съюз (Германия, Австро-Унгария и Османската империя).

Обективните реалности обаче твърде скоро превръщат САЩ в главен доставчик на военновременни материали за воюващите. Поради това още в края на 1914 г. тази нова реалност за пръв път дава основание на наблюдателите да определят Щатите като „крайъгълен камък“, от който ще зависи крайната военна победа. В резултат в хода на световната война САЩ постепенно се превръщат в арена на глобални дипломатически усилия. Борбата вече се води за това на чия страна в последна сметка ще застане и американската армия в бъдеще.

Дотогава българо-американските отношения се реализират активно, но главно в сферата на културата и образованието. През Възраждането американските протестантски мисионери съдействат за превода и издаването на Библията на новобългарски език. Впоследствие създаденото в Истанбул американско средно учебно заведение „Роберт колеж“ дава образование на няколко десетки млади българи. След погрома на Априлското въстание през 1876 г. американците Д. Макгахан и Е. Скайлер изиграват решаваща роля за запознаване на световната общественост с престъпленията на османската власт. С това те съдействат за спечелване на подкрепата на европейското обществено мнение в подкрепа на българите. След освобождението в България са изградени американски училища в Пловдив и Стара Загора, които също дават ценен принос в българската образователна система. През 1903 г. са установени и официални дипломатически отношения. За около едно десетилетие те се реализират от американска страна чрез легацията в Истанбул.

Победите на българската армия над Османската империя през Балканската война издигат авторитета на България и българите пред администрацията и общественото мнение в САЩ. А избухналата през 1913 г. Междусъюзническа война създава трайно впечатление в Северна Америка за една от най-големите неправди, извършени над даден народ през Новото време. За да оправдаят своите престъпни действия, правителствата в Белград и Атина обаче заливат световното обществено мнение с лъжи за „български зверства“, които били извършени през двете балкански войни. В тази връзка е формирана известната Карнегиева анкетна комисия с участието на учени от различни държави. Те проучват на място действителността, а след това публикуват изчерпателен доклад, разпространен в целия свят. В него учените доказват несъстоятелността на антибългарската пропаганда [3: 51 и сл.]. Рязката ескалация на вътрешнобалканската обстановка след Междусъюзническата война, както и очевидната реалност, че на Балканите предстоят нови, сложни политически процеси в перспектива, дават основание на правителството във Вашингтон да открие вече и Американско генерално консулство в София. През годините на Първата световна война длъжността „генерален консул“ се изпълнява от Доминик Мърфи.

При избухването на световната война през лятото на 1914 г. управляващите в София също осъзнават рязко повишената роля на „Америка“ за крайния изход от военния конфликт в бъдеще. Поради това Фердинанд и правителството на Васил Радославов решават да издигнат двустранните отношения между София и Вашингтон на ново равнище чрез откриването и на Българска легация във Вашингтон. За пръв пълномощен министър там е определен проф. Стефан Панаретов. Той е дългогодишен преподавател в американския „Роберт колеж“ в Истанбул и има широки връзки с американските дипломати и учени, работили на Балканите.

През септември 1914 г. проф. Панаретов се явява в София за консултации с управляващите. Там той провежда дълги разговори с цар Фердинанд и премиера Радославов. По време на аудиенциите са очертани основните цели на българската дипломатическа мисия в САЩ: да се положат максимални усилия, за да се стабилизира положителното отношение на президента У. Уилсън и на дипломатите в Държавния департамент към България и българите; да се направи всичко възможно за създаването на полезни връзки и с влиятелните медии в Щатите за отразяване на българската политика, като по този начин се надгради положителният резултат от Карнегиевата анкета; специално внимание да се обърне на издигането на ново, по-високо равнище на организационното състояние на българската емиграция в САЩ, за да се увеличи ефектът и от нейната обществено-политическа дейност сред американското общество; в резултат да се даде още по-сериозен и систематичен отпор на сръбската, гръцката и румънската антибългарска пропаганда в Америка, защото тя е подклаждана непрестанно от посланиците и разузнавателните служби на трите балкански държави, работещи във Вашингтон [4: 126].

След привършването на приготовленията, през ноември 1914 г., професор Ст. Панаретов, придружен от съпругата си и двамата секретари към легацията – Георги Пулиев и Христо Кънев, се отправят за САЩ. Българското дипломатическо пратеничество пристига в Ню Йорк на 6 декември 1914 г. С подкрепата на българския консул там – Клейтън Ракхил, Панаретов установява връзки с редакциите на някои от „главните вестници в Ню Йорк“. Техните журналисти проявяват жив интерес „да чуят нещо от мен, за моята мисия“, пише Панаретов в първия си доклад до София. „Всички изказаха удоволствие от отварянето на Българската легация във Вашингтон“ [4: 132 – 133], завършва докладът.

Придружен от консула Ракхил, проф. Панаретов пристига на 12 декември 1914 г. във Вашингтон. На 17 декември от 11.30 ч пълномощният министър се явява за пръв път в Държавния департамент. Там той връчва нотата, с която българското правителство информира държавния секретар по външните работи Бриян за акредитирането на българския пълномощен министър. Лидерът на американската дипломация посреща радушно първия български дипломат. Веднага урежда и аудиенцията му в Белия дом при президента У. Уилсън. Тя се провежда на 22 декември в 14.45 ч в Овалния кабинет. Там Панаретов връчва официално акредитивните си писма и резюмира основните цели на своята мисия: да съдейства за усилването на приятелските връзки между България и САЩ. Президентът Уилсън също подчертава значението на тази българска инициатива, защото тя издига на качествено ново равнище двустранните отношения между България и САЩ. В заключение Уилсън заявява: „В постигането на тези желания и благотворителни цели аз (Уилсън – бел. моя) ще съм особено щастлив да Ви окажа пълното си съдействие“ [4: 131 – 132].

Откриването на Българската легация на Кънектикът авеню и появата там на официален български пълномощен министър дава повод за ново активизиране на гръцката и сръбската пропаганда. За целите на своя антибългарски поход пълномощните министри на двете балкански държави използват платени агенти. Най-активно се изявяват журналисти от авторитетните американски вестници „Атлантис“ и „Дейли джърнъл“. За да се разсее антибългарската пропаганда, правителството в София планира най-напред посещение и на царица Елеонора в САЩ. Идеята е чрез организирането на срещи и разговори с видни обществени и културни дейци там тя да съдейства за намаляване на ефекта от пропагандата, реализирана отново от агентурата на Гръцката и Сръбската легация срещу България. Но рязко усложнилият се проблем с презокеанските пътувания по време на световната война постепенно правят невъзможна реализацията на тази контрапропагандна инициатива от българска страна. Поради

това прогръцкото лоби около редакцията на в. „Атлантис“ например няколко месеца препечатва едно антрефиле с радостния възглас: „Сбогом, Елеонора, сбогом!“. По този начин враговете на България изразяват радостта си от неосъщественото пътуване на царицата за намаляване на антибългарската пропаганда на балканската агентура, работеща в Съединените щати против България [4: 133].

При това положение след настаняването си в легацията Панаретов обсъжда с консула Ракхил как да се противодейства на гръцката пропаганда. Взето е решение да се установят най-близки контакти с редакцията на най-влиятелния вестник в САЩ – „Ню Йорк Таймс“. В тази връзка Панаретов поема инициативата и през декември 1914 г. провежда „няколко срещи“ с журналистите на това издание. Те получават подробна информация за неутралната политика, която България следва по това време в световната война; дават се много примери, доказващи колко високо управляващите в София ценят отношенията си с държавниците във Вашингтон; как и защо българите смятат американците за най-напредничавата нация на Новото време. Обоснована е тезата, че с откриването на Българската легация във Вашингтон САЩ също правят нова крачка напред в разширяването на своите политически позиции на Балканите и в Близкия изток. По този начин се увеличават възможностите, за да се реализират още по-активно и търговската дейност и политика от страна на Вашингтон в тази част на света. В резултат на което е постигнато споразумение Българската легация от този момент нататък да изпраща всяко свое съобщение или интервю на пълномощния министър най-напред на журналистите от „Ню Йорк Таймс“, за да може това издание първо да публикува съответната новина. Вследствие на това само този американски ежедневник получава копия и публикува пълния текст на словата, произнесени от Уилсън и Панаретов в Овалния кабинет при връчването на акредитивните писма [4: 134].

Узнал за дейността на българския пълномощен министър във Вашингтон, бившият американски президент Теодор Рузвелт изпраща на Панаретов наскоро публикуваната си мемоарна книга „Автобиография на Теодор Рузвелт“. Този факт също става известен на американското обществено мнение от страниците на „Ню Йорк Таймс“. В допълнение в началото на 1915 г. Панаретов провежда дълги аудиенции в посолствата на всички Велики сили, акредитирани във Вашингтон. По време на посещението си при руския посланик в САЩ Н. Бахметиев последният му съобщил, че при затегналата се война на Балканите отново се възраждала идеята за възстановяване на Балканския съюз от 1912 г. България обаче поставяла условие, че това може да стане само ако „Гърция върне територията на юг до гр. Кавала, а Сърбия се изтегли от Македония“.

Сведения и за тези визити и разговори стават известни чрез флагмана на американския печат „Ню Йорк Таймс“. Достойното посрещане на българския пълномощен министър във Вашингтон, официално изразеното уважително отношение към него от управляващите начело с президента У. Уилсън и влиятелни вестници, като „Ню Йорк Таймс“, отнемат почвата, върху която дотогава се реализира антибългарската пропаганда на балканската агентура зад океана. В резултат на това за около половин година активност гръцката и сръбската разузнавателна и дипломатическа служба в Съединените щати временно намаляват своята предишна агресивна антибългарска пропаганда. Стефан Панаретов получава възможност да реализира първата си обиколка из големите градове на САЩ, в които съществуват активни български емигрантски общности. След няколко срещи и разговори там с лидерите на отделните местни общности е подготвено провеждането на Третия редовен конгрес на Българомакедонския народен съюз [4: 138 – 141]. Решено е заседанията да се проведат в края на ноември 1915 г., защото тогава намалява работата по железопътното строителство, където са заети най-много от българите.

Междувременно през втората половина на 1915 г. обстановката на Балканите се променя съществено. Цар Фердинанд и правителството на Васил Радославов решават, че освобождението на българите в Македония може да се постигне по-сигурно чрез присъединяване на България към Тройния съюз, защото по време на преговорите с държавите от Антантата на българите се обещават промени на границите, но само след войната, когато вече е ясно какъв е реалният принос на българската армия в световния военен конфликт. Докато от Берлин заявяват, че „българско става веднага всичко, което си отвоюва българското оръжие“! При това положение през октомври 1915 г. Първа и Втора българска армия настъпват срещу сръбските войски в Македония. За по-малко от два месеца сърбите са принудени да се оттеглят през албанските планини на о. Корфу. Така през Първата световна война България става съюзник на Централните сили. Този факт активизира отново антибългарската пропаганда в Северна Америка до безпрецедентни мащаби, защото САЩ продължават да заемат неутрална позиция спрямо войната в Европа. По тази причина във Вашингтон работят легациите на всички европейски държави независимо от това, че едни членуват в Антантата, а други – в Тройния съюз, и са в смъртна схватка на бойното поле.

В новата обстановка антибългарската пропаганда в Северна Америка не само се активизира за пореден път. Тя обогатява и разнообразява и инструментариума, с който действа, и идеите, които лансира. Най-неочаквано проф. Панаретов е поканен на среща с австро-унгарския посланик във Вашингтон. В проведения доста напрегнат разговор представителят на Виена съобщава на българския пълномощен министър, че „добре информиран източник“ му е донесъл нещо важно: по време на интервюто, дадено от Панаретов след пристигането му в Ню Йорк, той бил заявил пред журналистите, че България много се е надявала преди началото на военните действия Сърбия да върне Македония на българите доброволно. Ако това станело (когато и да е), България била готова веднага да „даде военна помощ на Сърбия против Австрия“ [4: 135]. Стефан Панаретов отговаря, че нищо подобно не е казвал и че „добре информираният източник“, очевидно, разпространява невярна информация само за да влоши отношенията между България и Австро-Унгария. В доклада, който Панаретов изпраща до правителството в София, с основание прави извод, че в случая австро-унгарското разузнаване и дипломация просто „изпробват“ надеждността на новия си съюзник в световната война – българите. Факт е обаче, че Българската легация вече е обект на наблюдение и от службите на Тройния съюз, работещи в Америка.

След пълния разгром на Сърбия от българската армия сръбското правителство се настанява на о. Корфу. Поради липсата на финансови средства Сръбската легация във Вашингтон временно е затворена. Така за период от около две години този важен инсценировчик на антибългарска пропаганда в Съединените щати временно замлъква. В същото време обаче, отчитайки „липсата на надежден съюзник“ в антибългарската пропаганда, гръцкото разузнаване и дипломация се активизират по непознат в миналото начин. Схемата, по която се работи, е измислена изключително добре, като изпълнителите ѝ разчитат на пълното прекъсване на нормалните съобщения между България и САЩ в условията на световната война. В резултат на това разпространяваните фалшификации не могат да се проверяват веднага в София, за да се противодейства ефективно от страна на Българската легация.

Как действа конкретно гръцката агентура? Тя се състои от американски граждани с гръцко потекло. Те многократно са били в Гърция и на Балканите, така че познават много добре реалностите там. Разчитайки, че Българската легация не може да получава редовно и свободно информация от София, гръцкото лоби започва да публикува из американските вестници „новини“, почерпани уж от „вестниците, издавани

в София“. Най-често се цитират материали от проправителствения орган в. „Камбана“, и дори от народняшкия в. „Мир“. Една от най-активно натрапваната теза през есента на 1915 г. в платените статии, публикувани в някои американски вестници, е „германизацията на българите“. За да се увеличи ефектът от писаното, се привеждат цитати, представяни като извадки от вестниците, публикувани в София. Те били изпращани от „добре информирани източници“ в българската столица, въпреки че от октомври 1915 г. тези връзки са прекъснати напълно.

Многократно се интерпретира например информация, представяна като интервю, дадено от пълномощния министър на България в Берлин Димитър Ризов. Той бил казал: „Никога един владетел не е завладявал толкова бързо сърцата на един народ, както германският кайзер – българските сърца“. Целият български народ бил в „ентусиазъм“ (!?) от кайзера. Българите били трогнати особено от факта, че Вилхелм II подарил на тяхната родина „цялата военна плячка, взета от германските войски в Сърбия, на стойност от 30 до 40 милиона франка“. В отговор на казаното от Ризов третият син на кайзера – княз Август, дал също интервю. В него той признал, че „между германската и българската армия няма никаква разлика“. Поради това „Германия и нейният владетел и България винаги ще намерят кооперация и сътрудничество“ [1: бр. 220].

На тази основа авторите на антибългарските пропагандни материали правят извода, че отношението на германците е замъглило съзнанието на българите до такава степен, че те вече „сънуват да излязат от тази война като една световна сила и да се равняват с техните съюзници Германия и Австрия. Те не мислят да повърнат завладените територии“, твърди гръцкият агент. Без да се прави уточнението естествено в какви територии воюват българските армии на Балканите и какво население живее там. Като допълнителен аргумент се привежда цитат, извлечен уж отново от страниците на софийския в. „Камбана“. Авторът на пропагандната публикация твърди, че там пишело следното: „Със Сърбия разрушена и Румъния разделена България ще (...) удвои своите територии. Това също показва, че България ще бъде класифицирана в реда на Великите световни сили като независима държава, думата на която трябва да се слуша при регулирането на отношенията на нациите от целия свят“ [1: бр. 230].

Основната идея, която се натрапва на общественото мнение в САЩ, е, че България е новият „страшен агресор“ в Европа. На Балканите тя се бори не за постигане на националното обединение на своя народ, а за заграбването на чужди територии и население, само и само да се превърне в „световна сила“, така че тя да участва при регулирането на „отношенията на нациите от целия свят“. Целта е ясна: да се формира превратна представа сред американското обществено мнение по адрес на България и българите и по този начин да се влошат в перспектива официалните отношения между София и Вашингтон, така че на даден етап У. Уилсън да обяви война и на българите. Защото след влизането на България във войната дипломатическите отношение с държавите от Антантата са прекъснати. САЩ остават единствената Велика сила, с която България продължава да поддържа официални отношения до края на Първата световна война.

За да се удвои ефектът от повторно активизираната антибългарска пропаганда, платените агенти от Гръцката легация полагат сериозни усилия за компрометиране и на българската емигрантска общност в Съединените щати. Замисълът ѝ там е, че компрометирана, тя също ще загуби позиции в американското общество, за да не може да противодейства ефективно срещу инсинуациите на гръцката агентура. За да се придаде някаква адекватност на твърденията, отново се твърди, че „споменатите добре осведомени източници“ препратили в Съединените щати материал, който също бил почерпан от страниците на софийския в. „Камбана“. А текстът, който се твърди, че е

взет от там, има следното съдържание: „Единствените българи, находящи се засега в Америка, са вагабонти и банкови чиновници, които откраднаха чуждите пари в България и избягаха в Съединените щати, защото Съединените щати са страната, която протектира разбойници. Според една статистика сега в Щатите се намират около 12 000 българи. Досега нам не беше известно, че повече от тях са вагабонти и банкови крадци. Ето това е съюзницата на Германия, с която ние (САЩ – бел. моя) сега сме в мир“ [1: бр. 220]. Както се вижда, повече от коварно – „всички българи в САЩ са разбойници“. Самите САЩ според вестниците в София са „страна, която протектира разбойници“. Така мислели в София. Следователно как и българската общност в САЩ може да защитава интересите на България?

След влизането на България във войната обаче гръцката агентура в САЩ все пак отделя най-много време за фалшифициране на българската политика в новозавладените земи в Македония и Беломорието. Началото на тази пропагандна кампания е поставено с една фалшива телеграма „с дата 14-и юни 1917 г.“. Тя също била изпратена от „тогавашния гръцки пълномощен министър в София г-н А. Наум“. В нея се дават подробни фалшифицирани данни, според които правителството на В. Радославов изселило от Македония 5000 мюсюлмани. Те пристигнали в Пловдив, но след намесата на турския консул там били прехвърлени в Турция. Особено големи усилия българската военновременна администрация отделила и за намаляване на броя на гърците в населените меса по Беломорското крайбрежие, „за да се заличи гръцкият колорит на някои от областите, където той е преодоляващ“, твърди гръцкият агент [1: бр. 161].

Тъй като до пролетта на 1917 г. тази антибългарска пропаганда се води от името на „добре информирани източници“, без официални изявления на гръцкия пълномощен министър във Вашингтон, Ст. Панаретов решава, че е под неговото равнище да разобличава лично лъжите на гръцката агентура в Америка. Отговорните фактори във Вашингтон знаят, че от София тогава не могат да се получават тези материали, защото нормалната кореспонденция е ограничена. Така че писанията на гръцката агентура не провокират криза в българо-американските дипломатически отношения. Затова Панаретов се договаря с издателите на авторитетния български ежедневник в САЩ в. „Народен глас“ отговорите от българска страна да се дават чрез печата, но не от легацията, а от името на емиграцията. Ако Панаретов се ангажираше лично с тази невярна и платена информация, това би намалило излишно престижа на българския пълномощен министър сред американското общество, защото той би спорил за неверни неща с агентите на гръцкото разузнаване и дипломация в САЩ.

Издателите на в. „Народен глас“ поемат инициативата с ентусиазъм. С безспорни аргументи те разобличават една след друга всички лъжи на платената гръцка агентура в Съединените щати. Най-напред като абсурдни са определени твърденията за „германизацията на българите“. Като доказателство се привежда фактът, че българската армия се е намесила във войната не за да съдейства за реализацията на световните претенции на Германия да завладява други народи и да унищожава други държави, а само за да освободи своите братя, насилствено вкарани в границите на Сърбия и Гърция. Поради това нито един български войник не се е бил, не се бие и няма да се бие по фронтовете в Източна и Западна Европа, за да подпомага германците. Там основна действаща сила са германската и австро-унгарската армия. Следователно за каква „германизация на българите“ може да се говори?

По въпроса за „източниците на информация“, с които спекулира гръцката агентура, – споменатите български вестници, издавани в София, редакцията на в. „Народен глас“ доказва, че такива вестници действително съществуват. Но нито едно от тези патриотични издания в София не може и да си помисли (а камо ли да твърди

официално), че българската емиграция в Америка се състои само от банкови обирджии и крадци и че Щатите са техни закрилници! Как да е вярно това твърдение, след като то се хвърля като петно върху цялата българска емиграция!? По това време в САЩ живеят и работят към 50 000 българи. Всички те ли са обирджии и банкови крадци, питат българските журналисти? А що се отнася до твърденията, че гръцки посланик е съобщил от София „на 14 юни 1917 г." лъжите за демографското прочистване на небългарските елементи в Македония и Беломорието, българските журналисти в Съединените щати заявяват, че читателите просто трябва да се посмеят на глас, когато се докоснат до това невярно твърдение във вестниците. Защото след влизането на България във войната през октомври 1915 г. дипломатическите отношения между България и Гърция са прекъснати и в София няма гръцки посланик [1: бр. 161]. Как тогава въпросният „А. Наум" е изпращал доклади от София в Атина, за да стигнат те от там до САЩ? По тази логика на опониране в продължение на двете начални години от българското участие в Първата световна война българската общност в САЩ противодейства успешно на антибългарската пропаганда, реализирана от гръцката агентура.

Положението се променя съществено през зимата и пролетта на 1917 г. Февруарската революция в Русия прекратява активното присъствие на руската армия на Източния фронт. Съотношението на силите в Европа се променя в полза на Германия. При това положение след един много динамичен едномесечен дебат в Конгреса през април 1917 г. правителството на САЩ взема решение за влизане във войната на страната на Антантата. Американската армия се появява на Западния фронт срещу германските дивизии. У. Уилсън прекратява официалните дипломатически отношения с Германия, Австро-Унгария и Турция. България остава единствената държава от състава на Тройния съюз, на която не е обявена война. И американският президент, и дипломатите в Държавния департамент са наясно с коренно различните цели, които преследват в световната война, България и останалите Велики сили от състава на Тройния съюз. Въпреки това възниква качествено нова обстановка, в резултат на която през цялата 1917 г. в Конгреса и из печата тече дебат на тема все пак каква политика трябва да се провежда и по отношение на България, защото тя реално воюва в състава на противниковия военнополитически блок. От тази нова, сложна ситуация много бързо се възползва антибългарската агентура, подкрепяна от Гръцката, а вече и от Сръбската легация. След като САЩ влиза в световната война, Н. Пашич отваря отново сръбското дипломатическо представителство във Вашингтон.

„Българската тема" най-активно се обсъжда в Конгреса преди и след 9 април 1917 г. Инициативата подема конгресменът от Минесота Милер. В гневно изказване той заявява, че „представителите на България и Турция в Америка предават информация на неприятеля". Темата е подета и доразвита от председателя на Комисията по външните работи сенатора Ладж. Той „изказа своето негодувание – съобщава в. „Народен глас" – поради съществуването на такава легация в столицата (т.е. Българската легация – бел. моя). Той говори за нея като опасна за Америка и нейните съюзници, заявявайки, че тя трябва да бъде затворена и персоналът ѝ – заставен да напусне Вашингтон и страната изобщо" [1: бр. 296].

Темата е подета от някои вестници, спонсорирани от Гръцката и Сръбската легация. Отново и отново се развива пропагандната теза, че българите се стремят да разрушат съседните си държави, така че България да стане Великата сила на Балканите. Тази цел на управляващите в София била в пълен синхрон с германската доктрина за изграждане на т.нар. „Мидълевропа" – „Средноевропейски съюз", доминиран от германците след евентуалната им победа в световната война. Българските претен-

ции били израз на „патологичната агресивност и недемократичността на този балкански народ“. Българските действия обещавали Югоизточна Европа да се превърне в регион на „безкрайни военни конфликти в бъдеще“. От това нямало да има полза за нито един народ в света. Ето защо правителството на САЩ също трябвало да обяви война и на България и т.н., и т.н. В резултат на това фалшификациите по адрес на България и целите, които тя преследва в световната война, през 1917 г. отбелязват своята кулминация.

При това положение битката срещу тенденциозната антибългарска пропаганда е подета вече изцяло от пълномощния министър Стефан Панаретов. Той си налага практиката да посещава всяка седмица държавния секретар по външните работи Лансинг в Държавния департамент. Пред него Панаретов разяснява същността на българската политика. Основната теза, защитавана в Държавния департамент, гласи: целите, които България преследва в тази война, са същите цели, поради които и САЩ влязоха в световния военен конфликт – да се гарантират свободата и човешките права на всички хора, включително и на българите. А за да обоснове нейната същност, през 1917 г. Панаретов дава 15 интервюта и пише 25 статии, публикувани в „Ню Йорк Таймс“ и други влиятелни вестници [4: 158]. В срещите си с дипломатите в Държавния департамент и в материалите, излезли в печата, Панаретов развива една логична и убедителна теза. С нея той опровергава всички антибългарски изказвания в Конгреса и в статиите, писани из вестниците.

В известна последователност неговите изложения в печатните медии следват следната логика: пълни фалшификации на истината са твърденията, че Българската легация във Вашингтон изпраща секретна информация до правителствата на държавите, съставляващи Тройния съюз, защото след влизането на България във войната през есента на 1915 г. пряката връзка на Българската легация във Вашингтон с Външното министерство в София е прекъсната. Поради това, когато пълномощният министър изпраща свой доклад до българското правителство, това той върши чрез куриерската служба на американското Външно министерство. Особено показателен в това отношение е случаят със смъртта на царица Елеонора през 1917 г. Дори тогава съболезнованията на Панаретов до царя в София са изпратени чрез американската дипломатическа служба. Пак тя връща и благодарствения отговор на Фердинанд по повод на изказаните му съчувствия във връзка с трагичния случай [1: бр. 295].

Освен това България няма във Вашингтон военно и военноморско аташе, така че няма кой да събира и изпраща съответната информация за приготовленията и действията на американската армия и флот. Положението по фронтовете също доказва, че няма причини за скъсване на дипломатическите отношения между САЩ и България. Най-напред, защото българската армия е разположена само на Балканския фронт на военните действия. Основната цел на българите, преследвана там, е освобождението и обединението на насилствено откъснатата част от техния народ през Междусъюзническата война. **„Почти цялата наша армия от 900 000 човека се намира в Македония, сражавайки се за възвръщането на България територията, която несправедливо бе отнета от нея, на края на втората балканска война. Това е всичко за което се бием и възнамеряваме да се бием и занапред, ако е нужно. Ние не сме заинтересувани от някакви планове за „Мидтелевропа“** (Средна Европа) **нито пък се стараем за някаква хегемония на Балканите. Ние сме против абсолютизма, на всяка крачка“** [1: бр. 296] – това заявява Панаретов в много от своите статии.

Така твърденията на сръбската и гръцката агентура, че България ще създава някаква „Велика сила“, подобна на Германия, са квалифицирани като пълна фалшификация на истината. В допълнение Панаретов многократно обяснява, че на Западния фронт, където действа вече и американската армия, не е имало, няма и няма да има

никога нито един български войник, а на Балканите няма американски войски. И не съществува никаква възможност за пряк военен конфликт между въоръжените сили на България и САЩ, така че да се наложи скъсване на дипломатическите отношения между София и Вашингтон. Освен всичко друго, България не разполага и с военноморски флот и подводници в Атлантика – средства, с които евентуално биха могли да се поставят под заплаха американските комуникации през океана и така също да се влошат доставките за американската армия на Западния фронт [1: бр. 296].

Освен това българското правителство не се поддава на силния натиск, упражняван от страна на кайзера и германското правителство, за скъсване на дипломатическите отношения между САЩ и България. „България се характеризира в тая страна (САЩ – бел. моя) от някои членове на Конгреса като оръдие и подвластна държава на Германия. Това е абсолютно невярно – заявява Панаретов в едно от своите интервюта. – Ако ние бяхме подвластна на Германия държава, то защо не скъсахме дипломатическите ни връзки със Съединените щати, както германското правителство ни подбуждаше? Германия употреби всичкото си влияние върху България (...) за да скъса отношенията си със Съединените щати. Обаче ний постоянно сме отказвали да удовлетворим това нейно желание, по простата причина, че няма причини, за да влизаме в конфликт със Съединените щати. Когато бяха скъсани връзките между Щатите и Австрия, аз отидох в министерството на външните работи и се видях с г. Лансинг – продължава Панаретов. – Запитах го: „Г-н Лансинг, къде стои България?“. Той отговори, че ний стоим „там, където сме стояли и преди“ [1: бр. 296], т.е., че правителството на САЩ смята да продължава съществуването на двустранните дипломатически отношения, без да се обявява война и на България.

На този фон благоприятно влияние върху позицията на президента Уилсън и Държавния департамент във Вашингтон във връзка с бъдещето на българо-американските отношения оказват и изключително добронамерените и обективни донесения на американския генерален консул в София Доминик Мърфи. Българското военно разузнаване успява да се снабди с превод на неговия Доклад № 175, от 25 май 1917 г. В този официален документ Мърфи много подробно разказва за положителното отношение на българите към САЩ, градено през десетилетията и с ролята на Скайлер и Макгахан при разкриването на турските зверства през 1876 г., и чрез влиянието, което „Робърт колеж“ в Истанбул има за подготовката на българската интелигенция [2: 422 – 428].

Във въпросния доклад Доминик Мърфи поставя обаче особен акцент върху категоричната позиция на България, че правителството на В. Радославов няма никакви намерения да обявява война на САЩ въпреки изключително силния натиск от страна на официален Берлин в това направление. В доклада си Мърфи разказва и за аудиенцията, която е поискал при В. Радославов на 10 май 1917 г. „Целта ми беше – пише Мърфи – да мога да науча от самия председател истинското положение, защото се знае положително, че в германските и австрийските кръгове се очаква едно бързо скъсване на отношенията (между България и САЩ – бел. моя). Моят прием бе посърдечен от обикновено (...) и имах голямото удоволствие да получа положително уверение, че добрите отношения между България и САЩ няма да бъдат нарушени. Министър-председателят ме увери за неговата лична висока оценка на американското правителство и за неговото ревностно желание, което е и желание на неговия народ, да запази това приятелство“ [2: 422 – 428].

В резултат на активната защитна политика, реализирана от Стефан Панаретов във Вашингтон, и приноса, даден от Доминик Мърфи от София в подкрепа на отстояваната теза за добрите българо-американски отношения, едногодишната антибългарска пропаганда, инсценирана от гръцката и сръбската агентура в Съединените щати не дава очаквания резултат. На 24 април 1918 г. в. „Народен глас“ обобщава резултата

по следния начин: „Днес в една конференция в Сената, със сенаторът Кинг от Юта, президентът Уилсън се изказа окончателно против обявяването на война на България (...) от Съединените щати (...) Причините, по които президента не желае обявяването на война на поменатата държава не се съобщават. Обаче сенаторът Кинг, след срещата си с президента заяви, че няма да настоява за прокарването на предложението си“ [1: бр. 291] за обявяване на война срещу България.

Причината е известна: и президентът Уилсън, и Държавният департамент заявява в Сената, че „случаят с България е друг“. Правителството и народът на България се стремят чрез участието в световната война да отстранят тежестите, стоварени върху българите в Македония през грабителската Междусъюзническа война от 1913 г. В резултат на това до края на Първата световна война през ноември 1918 г. България остава единствената държава от състава на Тройния съюз, с която американското правителство запазва официалните си дипломатически отношения непокътнати. Нещо повече – по време на преговорите за примирие, проведени в Солун, между българското пратеничество и представители на Антантата през септември 1918 г. Доминик Мърфи придружава българската делегация. Там той съдейства за по-бързото подписване на споразумението за прекратяване на военните действия и излизането на България от Първата световна война. В хода на преговорите за мир в Париж през 1919 г. американската делегация настоява за присъединяването към България на някои територии в Македония, населени предимно с българи. Тъй като английската и френската делегация не приемат тази идея, след подписването на Ньойския договор за мир на 27 ноември 1919 г. правителството и Конгресът на Съединените щати единствени не ратифицират (т.е. не признават) клаузите на този антибългарски диктат, наложен вече по волята на европейските велики държави.

* * *

Така приключва една от най-тежките и успешни битки, водени от българската дипломация срещу антибългарската агентура на сръбската и гръцката дипломация в Съединените щати. Благодарение на решителното и добре аргументирано противодействие на българския пълномощен министър във Вашингтон проф. Стефан Панаретов по най-убедителен начин е доказана несъстоятелността на пропагандните клишета. И въпреки невероятно сложната обективна среда, в която България и САЩ воюват в състава на двата противоборстващи си лагера в Европа, двустранните отношения между София и Вашингтон оцеляват до излизането на България от войната. В крайна сметка е написана една от най-интересните и поучителни страници на българо-американските политически отношения в историята на борбата, водена от българската дипломация през Новото време срещу разузнаванията и пропагандите на антибългарски фактори в международните отношения. Поуките от нея могат да служат и днес, и в бъдеще на управляващите в София, когато отношенията между САЩ и ЕС също навлизат в нова и неизвестна фаза на своето бъдещо развитие.

Литература

1. ***В. „Народен глас“,*** бр. 220 от 18.09.1917 г.; бр. 291 от 24.04.1918 г.; бр. 295 от 17.12.1917 г.; бр. 296 от 18.12.1917 г.; бр. 230 от 29.09.1917 г.; бр. 161 от 26.07.1918 г.
2. **Малеев,** Лука. Моето адютантство. София, б.д.
3. **Митев,** Тр. Спонтанният пробългарски лобизъм в САЩ, провокиран от Карнегиевата анкета комисия (1913 – 1914 г.). – В: *Военноисторически сборник,* 1997, кн. 3.
4. **Митев,** Тр. История на Българския емигрантски патриотичен фронт в Новия свят (края на XIX – края на XX век). Част 1. София: Държавна агенция за българите в чужбина, 2021.
5. **Пантев,** А., П. Петков. САЩ и България по време на Първата световна война. София: Наука и изкуство, 1983.

ИНОВАТИВНИ РЕШЕНИЯ ЗА РАЗВИТИЕ НА ЛИДЕРСТВОТО В ОРГАНИЗАЦИИТЕ ОТ СИСТЕМАТА НА НАЦИОНАЛНАТА СИГУРНОСТ

проф. д-р Валентин Василев
Висше училище по сигурност и икономика – Пловдив

INNOVATIVE SOLUTIONS FOR LEADERSHIP DEVELOPMENT IN ORGANIZATIONS OF THE NATIONAL SECURITY SYSTEM

Prof. Valentin Vasilev, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Ролята и интересът към значимостта на „сигурността“ във всичките ѝ аспекти през последните години се увеличава като снежна топка. Прецизният прочит и анализ на тези процеси безспорно могат да насочат вниманието ни към една от ключовите области в този процес – ролята на човешкия фактор. В такъв контекст представеният доклад резонира с предизвикателствата на осъзнаването на ролята на лидерството и лидерските качества в процесите на подготовка и реализация на ключови политики в областта на националната сигурност на всички равнища. В разработката акцент се поставя на ролята на съвременните концепции за лидерство в системата на сигурността, както и се извеждат някои ключови идеи за подобряване на този процес в управленските парадигми, прилагани в системата на националната сигурност.*

Ключови думи: *сигурност; лидерство; институционално развитие; кризи; човешки ресурси; мотивация; емоционална интелигентност*

Abstract: *The importance security in all of its aspects and the role that it plays have grown like a snowball in recent years. One of the most important aspects of this process – the function of the human factor – can surely be brought to light by carefully reading and analyzing these procedures. In light of this, the paper highlights the difficulties in recognizing the importance of leadership and leadership qualities in establishing and carrying out important national security policies at all levels. The importance of contemporary leadership concepts in the security system is developed, along with some important suggestions for enhancing this procedure in the management paradigms used in the national security system.*

Key words: *security; leadership; institutional development; crisis; your resources; motivation; emotional intelligence*

Въведение

Лидерството в настоящия момент се явява един от най-важните управленски инструменти в развитието и дейността на организациите. Не е случаен фактът, че развитието на лидерски умения е залегнало в редица нови стратегически документи, засягащи работата на публичния сектор, и по-точно – в органите и институциите, пряко ангажирани с националната сигурност.

Макар и бавно, повишеното внимание към проблематиката, свързана с лидерските аспекти на работата, извеждат на преден план широк спектър от проблеми и предизвикателства от различен характер. Неслучайно ООН промотира човешката сигурност като мощен подход с траен ефект спрямо най-сериозните дефицити на мира и развитието. „Двигателят“ на човешката сигурност се запалва от самите хора – от

техните нужди, потребности, предизвикателства. Несигурностите, които ги заплашват, изискват обединени и всеобхватни действия за борба с тях, както и сътрудничество и партньорство на всички нива (във вертикално отношение) и между различни партньори и заинтересовани лица и групи (в хоризонтална мрежа) [8: 149].

Настоящата разработка прави опит да представи, от една страна, някои нови тенденции и идеи в теоретичното рамкиране на лидерството [11: 585], а от друга страна, да насочи вниманието на читателите към спецификата на обучението и развитието на лидерство в системата за национална сигурност.

Съвременни теоретични детерминанти за осмисляне на ролята на лидерството

Както отбелязва Клаус Шваб във фундаменталната си разработка „Четвъртата индустриална революция“, „…понастоящем промените са исторически по отношение на своя размер, скорост и обхват“ [10: 22]. Променливи са и човешките общества – икономическият живот, културата, ценностите, дейностите. Промяната е в нас и около нас. Затова ние трябва да я възприемем като необходимост и да се научим да я управляваме ефективно.

С нарастване на информационния поток, повишаване на изискванията към организацията на административната дейност и за достигане на добра производителност в работата е необходимо методично и целенасочено да се работи за внедряване на новите технологични решения и усъвършенстване на информационната среда в контекста на адаптиране на организацията към съвременните концепции за информационно общество и развитие на онлайн пространството, включително и към „фината“ настройка към промените в обществото на всички равнища.

Лидерството е сложен процес, с подчертано практическо значение и несъмнено заслужава задълбочено изучаване и дълго време се изследва в два аспекта – като процес и като свойство [16].

Според Марк Бракет „Нашият емоционален живот е влакче в увеселителен парк, което се изкачва високо в един момент и се спуска стремглаво в следващия (...) нашето емоционално състояние е един от най-важните аспекти на нашия живот. То управлява всичко останало и влиянието му е всеобхватно“ [1: 34].

С настъпилия напредък в психологическите и управленските науки то започва да се изследва и като процес и свойство едновременно. Това поражда определянето на лидерството в три направления:

- като свойство – лидерството е множество от специфични характеристики, притежавани от тези, които го упражняват успешно;
- като процес – лидерството е пряко непринудително влияние и координиране на действията на групата по пътя към достигане на нейната цел;
- едновременно като процес и свойство – лидерството е пряко непринудително влияние на лица, които притежават съответните качества за достигане на определена цел.

Представените теоретични рамки са индикативна основа за възприемане на идеите за развитие на лидерството, които ще представим по-долу.

Решения за развитие на лидерството в организациите от системата на националната сигурност

Реформите в мениджмънта не са подминати от световните тенденции на промени в цялостната икономическа обстановка. От друга страна, ако пандемията от Ковид-19 ни научи на нещо, то е, че начините, по които работим, как се съсредоточаваме върху нашите хора, подкрепяме благополучието и приобщаването им, иновациите и адаптацията им, могат да се променят към по-добро.

Мениджмънтът претърпява съществена еволюция от гледна на точка на променящите се и глобализиращи се пазари и се ориентира към иновативни и практически насочени действия, с основна цел адаптация към променящата се среда, в която работят организациите [4: 176]. В допълнение към тези предизвикателства е необходимо да се отбележи и специфичният акцент, който указват различните аспекти в областта на сигурността и защитата на правата на човека, разгледани в контекста на управлението на персонала в глобализираща се среда, като се дефинират като общозадължителни за всички държави в епохата на глобализацията основни положения [17].

Новите подходи в управлението набират сила в повечето развити държави през последното десетилетие и обхващат сферата както на общия мениджмънт, така и на обществените услуги и сигурността [4]. Основният подтик, предизвикан от промените през последните „пандемични“ и кризисни години, се изрази в признаване на обстоятелството, че подобренията в ефективността на организациите са тясно свързани с човешкия фактор, а оттам и с практиките по мотивиране, подбор, оценка на потенциала и мениджмънта на талантите, работни методи, отношения с персонала, мотивационна политика и други аспекти на мениджмънта на персонала и лидерството.

Емоционална интелигентност и значението ѝ за лидерството в сигурността

Емоционалната интелигентност е организирана уникална за човека система от осъзнати емоции, способности, компетентности и личностни характеристики. Тя е комплексното знание на човека за механизма и процесите, по които той чрез емоциите си управлява себе си, поведението си и взаимодейства с другите. Всеки човек има различно ниво на емоционална интелигентност. То се определя от генетичната унаследеност от родители, от ниво на осъзнатост, от придобити умения и развити способности през периоди на учене. Тя не е статична константа. Емоционалната интелигентност е модел на осъзната емоционална саморегулация и не може да се копира, а е нужно да се самоизгради [7: 273].

По този начин всеки служител се чувства ценен и желае да расте заедно с организацията, в която работи. Терминът „ЕИ“ е определян от Американското дружество по диалектика като най-новия и често използван в научната литература през 1995 г., а през годините значително утвърди присъствието си в научната и практическата лексика и управленска стилистика [9].

Основната идея на емоционалната интелигентност включва възприемането, разбирането, използването и управлението на личните емоции, както и на емоциите на други хора. Освен себе си като емоционално интелигенти хора, е необходимо да можем да разбираме мотивациите на другите, както и техните цели и чувства [3].

Развитието в тези области прави лидерите по-продуктивни и по-мотивирани и същевременно има подобен ефект върху хората, с които се работи. Като цяло организациите, които са „емоционално интелигентни“, са по-стабилни и имат по-лоялни служители и клиенти [2: 111].

Можем да обобщим също така, особено в контекста на сигурността и кризисния мениджмънт, че ЕИ понастоящем е ключов инструмент за реакция в ситуации от различно естество, включително и в областта на особено значимите и придобиващи пандемични размери киберпрестъпления и киберагресия [14].

Според редица водещи световни експерти успехът на човека се определя не толкова от неговия коефициент на интелигентност (IQ), колкото именно от нивото му на емоционална интелигентност. Успешният лидер никога не упреква никого и нищо за емоциите, които изпитва. Той владее собственото си съзнание и се учи да не реагира „емоционално“. В този смисъл едно от най-мъдрите решения, които би могъл да вземе едни мениджър, е да започне да развива своята емоционална интелигентност, така че да се превърне в по-добър лидер.

Бредбъри и Грийвс – автори на книгата „Емоционална интелигентност 2.0“, предлагат начин, по който можем да разпознаем хората с висок EQ. През последните години все по-често се обсъжда т.нар. „емоционален интелект“ – параметър, използван, за да се попълни липсващото звено, подсказвано от откритието, че хората със среден коефициент на интелигентност (IQ) в 70 % от случаите се изявяват по-добре от тези с най-високо ниво на IQ. Изследвания, провеждани в продължение на десетилетия, показват, че емоционалният интелект е един от най-важните фактори за професионален успех – 90 % от най-ценните сътрудници притежават висок EQ. Всеки от нас притежава емоционален интелект – т.е. „нещо“ нематериално, което влияе на нашето поведение, социализация, умения за вземане на решения с цел постигане на положителни резултати [18]. Нематериалната природа на EQ обаче не ни позволява да го измерим особено точно, за да разберем как можем да го подобрим. Бредбъри предлага един начин, по който можем да разпознаем хората с висок EQ. Той е анализирал данните от изследване на компанията TalentSmart, проведено сред 1 млн. души, и е откроил типовете поведение, които издават високо ниво на EQ. Ето какви са те: Богат емоционален речник; Интерес към хората и положителна нагласа към промените; Познаване на собствените слаби и силни страни; Разбиране на другите и умение за даване; Неуязвимост на обиди; Умението да се казва „не“ (на себе си и на други); Балансирано отношение към грешките; Умение за абстрахиране; Неутрализиране на вредните хора; Контролиране на амбициите и позитивизъм; Самооценка.

Емоционалната интелигентност е подходящ управленски инструмент за развитие на лидерство в системата на сигурността и всички индикации са, че интересът към ЕИ е голям и се увеличава.

Мотивация и мотивационни техники. Приложение на модела „Мотивация 4.0“ в лидерството

На основата на направено практическо изследване (2021 – 2022) Василев и Ичева извеждат модела „Мотивация 4.0“ [15: 247], който се апробира в публичната администрация и към който интересът понастоящем е много голям в институции и организации от публичния сектор. Този модел и елементите в него са в чудесна релация с концепцията за лидерство в системата на сигурността, като допълват по подходящ начин ключовите идеи от концепцията за развитие на лидерство.

Основни елементи на модела са: *социалната отговорност, зеленото управление на човешките ресурси, бенчмаркингът и емоционалната интелигентност*. Разработването и прилагането на политики в тези четири области са ключови за повишаването на мотивацията на служителите, както и могат да се отразят върху изграждането на лидерски умения и компетенции.

Упражняването на ***корпоративната социална отговорност*** се разбира като съществена възможност за повишаване на конкурентното предимство, като позитивира корпоративната репутация [6]. В контекста на функционирането на публичната сфера следва да посочим, че все по-често се налага общините да бъдат в конкуренция помежду си при нуждата от финансиране на определени проекти. Концепцията за корпоративната социална отговорност е стратегически свързана с иновациите чрез създаване на икономически и социални ценности, които създават устойчиво мотивационно въздействие в организацията [13: 166]. Със своята дейност организациите следва да намерят своя отличителен белег, конкурентно предимство и приноса, който имат в развитието на областта, в която се реализират, но и във функционирането и подобряването на средата за живот, в която функционират.

Друг компонент в модела е т.нар. ***„Зелено управление на човешките ресурси (ЗУЧР)“.*** То се свързва с устойчивостта, опазването на околната среда и отговорността ни към нея. В контекста на управленския процес зеленият мениджмънт може да бъде включен във всички функции на човешките ресурси – от подбора, през социализацията, до мотивацията на служителите. Например при реализирането на подбора все повече се предпочитат методите, които предлагат информационните технологии. Това са онлайн подаване на документи за кандидатстване за дадена позиция чрез различни уеббазирани платформи, сайтове или електронни пощи. Зеленото в управлението на човешките ресурси може да бъде използвано и в други функции, като възможностите за неговото широко прилагане са изключително добре възприемани, особено от новото поколение служители [5: 145].

Все по-често използван управленски инструмент за реализиране на публични политики в областта на мотивацията е ***бенчмаркингът.*** Терминът „бенчмаркинг“ е англоезичен. Той произхожда от думата *„benchmark“,* която означава *„белег“, „знак“* на фиксиран обект. В най-общия смисъл това е нещо, притежаващо определено количество, качество и способност да бъде използвано като стандарт при сравняване с други подобни. Бенчмаркингът е елемент от мотивационния процес, тъй като е свързан с автомотивация [12]. Вътрешното ни желание за нови знания, умения, прогрес ни води към търсенето на нови подходи, които да ни направят по-добри служители. До голяма степен използването на този инструмент зависи от стила на ръководство на ръководителя и неговата нагласа към промяната, иновациите и развитието. Апробирането на доказано добри практики е доказан инструмент за разширяване на ефекта от търсенето на иновативни начини за намиране на решения в различни управленски ситуации.

От друга страна благоприятната служебна обстановка е свързана с наличието на ефективна комуникация между отделните служители, както и между служителя и ръководството, с липсата на конфликти и стрес, със спокойствие и ефективност. До голяма степен тези фактори зависят не само от ръководителя на организацията, но и от отношението на всеки един от служителите. Поради тази причина все по-актуална става темата, свързана с ***емоционалната интелигентност, която е четвъртият компонент в модела „Мотивация 4.0“, за която вече писахме по-горе в настоящия доклад.*** Понятието е сравнително ново и през последните години представлява

интерес и обект на изследване в редица научни статии и трудове, като безспорно доброто използване на предимствата на емоционалната интелигентност е в пряка връзка с мотивацията и с развитието на лидерски характеристики.

Заключение

Разбира се, безспорно може да се подчертае важността на лидерството във всеки управленски процес и решение. То се простира отвъд границите на ежедневното целеполагане и ефективност, като се свързва с визия и мисия на организациите. Нещо повече – от лидерството в огромна степен зависят цялостното организационно развитие и динамика на ефективност при изпълнение на стратегическите и оперативните цели във всяка организация.

Приложението на добри практики при развитието на лидерството, и особено на такива в областта на управлението на човешките ресурси, в дългосрочен план безспорно ще се отрази на общата ефективност на организациите, като това е особено валидно за тези от областта на националната сигурност. Представените идеи могат да бъдат начало за осмислени подходи и политики, свързани с мотивацията и развитието на човешките ресурси и да се използват като фундамент, върху който да се надградят организационни практики в посока на търсене на устойчиви резултати в областта на развитието на човешкия капитал в структурите от областта на националната сигурност.

Литература

1. **Бракет,** М. (2024). Позволението да чувстваш. София: Фреи.
2. **Василев**, В. (2021). Съвременни мотивационни техники в мениджмънта. София: Пропелер.
3. **Василев,** В., Цв. Бельовска. (2017). Възможности за приложение на емоционалната интелигентност в публичната администрация. – В: Годишник на Нов български университет (НБУ), Департамент „Администрация и управление“, Том I, 2017. [онлайн]. *https://www.ceeol.com/search/article-detail?id=682171.*
4. **Димитрова,** И. (2023). Енергийните кризи като фундаментална заплаха за сигурността. – В: *Сборник* с доклади от научната конференция „Актуални проблеми на сигурността“ на НВУ „Васил Левски“, 26 – 27.10.2023 г., том 5, с. 173 – 182. ISSN 2367-7465.
5. **Илиева,** Н., В. Василев. (2022). Зелено управление на човешките ресурси, мотивация и лидерство – от иновации към традиции и добри практики. – В: *Сборник* с доклади от международната научна конференция „Изкуственият интелект в сферата на сигурността – предимства и заплахи“ (Докторанти и студенти), ВУСИ – Пловдив, 30.09.2022 г., с. 145 – 152. ISBN 978-619-7343-71-7. [онлайн]. *https://www.ceeol.com/search/chapter-detail?id=1113807.*
6. **Ичева,** М., Д. Огнянски, В. Василев. (2022). Ролята на социалната отговорност в мениджмънта на кризи – от организационен редизайн към устойчиви практики. – В: *Публични* политики, том 14, № 1. [онлайн]. *http://www.ejpp.eu/index.php/ejpp/article/view/4.*
7. **Кардашева,** А., В. Василев. (2022). Емоционална интелигентност и организационно развитие – добри практики и решения в кризисни времена. – В: *Сборник* с доклади от международната научна конференция „Изкуственият интелект в сферата на сигурността – предимства и заплахи“, ВУСИ – Пловдив, 30.09.2022 г., с. 273 – 278. ISBN 978-619-7343-71-7. [онлайн]. *https://www.ceeol.com/search/chapter-detail?id=1113139.*
8. **Сидова,** Д. (2023). Политическата сигурност като измерение на свободата от страх в контекста на човешката сигурност. – В: *Сигурност* и отбрана, декември 2023, бр. 2, с. 149 – 161. [онлайн]. *https://doi.org/10.70265/ACKH6038.*
9. **Стефанова,** Д., В. Василев. (2022). Ефективна лидерска комуникация в мениджмънта на кризи – в търсене на комплексен модел с фокус към бъдещето. – В: *Сигурност* и отбрана, ноември 2022 г., бр. 1, с. 103 – 110. [онлайн]. *https://institute.nvu.bg/bg/node/24.*
10. **Шваб,** К. (2016). Четвъртата индустриална революция. София: Хермес.

11. **Bahuguna,** P. C., R. Srivastava, S. Tiwari. (2023). Two decade journey of green human resource management research: A bibliometric analysis. – In: *Benchmarking:* An International Journal, 30(2), pp. 585-602.
12. **Chamizo-Nieto,** M. T., L. Rey, J. Pellitteri. (2020). Gratitude and Emotional Intelligence as Protective Factors against Cyber-Aggression: Analysis of a Mediation Model. – In: *J* Environ Res Public Health, 2020, Jun 22, 17(12):4475. doi: 10.3390/ijerph17124475. PMID: 32580331. PMCID: PMC7345504.
13. **Gigauri,** I., V. Vasilev, D. Sidova. (2025). The Role of Leadership and Corporate Social Responsibility for Sustainable Entrepreneurship: Good Practices From Georgia and Bulgaria. – In: *Sustainable* Entrepreneurship and Family Business for Women's Empowerment. I. Gigauri. (Ed.). IGI Global Scientific Publishing, pp. 165-176. [online]. *https://doi.org/10.4018/979-8-3693-8694-1.ch008.*
14. **Gigauri,** Z. (2025). Why Is Corporate Social Responsibility Necessary?: Public Awareness Survey in Georgia. – In: *Navigating* Corporate Social Responsibility Through Leadership and Sustainable Entrepreneurship. Iza Gigauri and Ali Junaid Khan. (Eds.). IGI Global, 2025, pp. 57-82. [online]. *https://doi.org/10.4018/979-8-3693-6685-1.ch003.*
15. **Icheva,** M., V. Vasilev. (2021). The time for the next steps is here – from classic to modern paradigms in motivation. – In: *International* Journal of Social Science & Economic Research (IJSSER), vol. 6, No. 3 (March 2021). ISSN 2455-8834. [online]. *https://ijsser.org/more2021.php?id=58.*
16. **Serafimova,** V., H. Dissanayake, A. Iddagoda, V. Vasilev. (2025). Inclusive Leadership and Corporate Social Responsibility for Women's Empowerment: From Good Ideas to Sustainable Solution. – In: *Sustainable* Entrepreneurship and Family Business for Women's Empowerment. I. Gigauri (Ed.). IGI Global Scientific Publishing, pp. 177-202. [online]. *https://doi.org/10.4018/979-8-3693-8694-1.ch009.*
17. **Vasilev,** V., M. Icheva. (2023). In search of solutions for employee motivation – from ideas and good practices to working models. – In: *Journal* of Management Sciences and Applications, 2(2), pp. 248-254. [online]. *https://jomsa.science/index.php/jomsa/article/view/59.*
18. **Yaneva,** Dilyana, Vesela Serafimova. 2020. Increasing corporate image by the employment of disabled people. – In: *Revista* Inclusiones, agosto, 2020, p.p. 170-79. [online]. *https://www.revistainclusiones.org/index.php/inclu/article/view/1749.*

ПРОДОВОЛСТВЕНАТА СИГУРНОСТ В КОНТЕКСТА НА СЪВРЕМЕННОТО РАЗУЗНАВАНЕ (НА ПРИМЕРА НА АНКЕТНО ПРОУЧВАНЕ)

проф. д-р Валери Велковски
Висше училище по сигурност и икономика – Пловдив

FOOD SECURITY IN THE CONTEXT OF MODERN INTELLIGENCE (USING THE EXAMPLE OF A SURVEY)

Prof. Valeri Velkovski, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *В световен и национален план продоволственият проблем обхваща множество направления, свързани с пълноценното в количествено и качествено отношение изхранване на населението. Стратегическата роля на продоволствената сигурност включва поддържане на удовлетворителни параметри на продоволствената програма и свързаните с нея основни характеристики на земеделието и аграрния сектор. От гледна точка на държавната политика в аграрния сектор е необходимо да се използва при поддържането на необходимите параметри на продоволствената сигурност инструментариумът на разузнаването.*

Ключови думи: *продоволствен проблем; продоволствена сигурност; разузнаване; земеделие; аграрен сектор; държавна политика*

Abstract: *On a global and national level, the food problem encompasses many areas related to the complete quantitative and qualitative nutrition of the population. The strategic role of food security includes maintaining satisfactory parameters of the food program and the related basic characteristics of agriculture and the agrarian sector. From the point of view of state policy in the agrarian sector, it is necessary to use the tools of intelligence in maintaining the necessary parameters of food security.*

Key words: *food problem; food security; intelligence; agriculture; agrarian sector; state policy*

Въведение

Продоволствената сигурност е пряко свързана с продоволствения проблем – проблем, който съпътства човечеството от зората на човешката цивилизация до наши дни. В съвременния свят усложняването на продоволствения проблем се влияе от редица фактори, сред които т.нар. „глобален демографски проблем“, който отразява ускорената демографска популация, или т.нар. „демографски срив“, чиито статистически измерения достигат цифрата 8 млрд., с тенденция до 2050 г. населението на планетата да се увеличи до 9 млрд. души. Това създава сериозни проблеми в изхранването на населението, особено в някои географски ареали, където демографската популация е особено активна.

За да се осигури храна на населението, обемът на продукцията трябва да се увеличи със 70 %.

Както посочват някои анализи, „37 % от земната повърхност се използва за селско стопанство. Около 52,5 млн. кв. м се разпределят за пасища. На 7,2 млн. кв. км се отглеждат земеделски култури“ [2: 2].

Каква е ситуацията у нас?

Според преброяването на земеделските стопанства през 2020 г. и показаните резултати [1: 2] използваната земеделска площ възлиза на 4 564 152 ха, а обработваемата земя е с площ 3 317 071 ха. Зърнено-житните култури заемат 1 986 895 ха. Най-голяма площ в тази група заемат обикновената пшеница и лимецът – 1 201 667 ха, а най-малка е площта с ръж – 228 ха. От основните култури, които влизат в основния продоволствен пакет на българина, оризът заема 12 491 ха, зърнено-бобовите култури – 24 821 ха, картофите – 11 721 ха, и т.н.

Посочените площи и добивите от тях са в пряка зависимост от климатичните фактори и проблема с някои природни ресурси – например водата.

Както посочват други автори, „производството на земеделски хранителни продукти в съвременната икономика е изправено пред значими обществени предизвикателства, свързани с решаването на редица икономически, социални, екологични и управленски въпроси. От една страна, се търсят отговори за нарастване на устойчивостта на стопанствата и удовлетворяване на нуждите на потенциалните потребители от достъпна и качествена храна, а от друга – да се повиши добавената стойност чрез преработка на произведените суровини“ [4: 2].

Продоволствената сигурност трябва да отразява и променящите се потребителски тенденции, които, както отбелязват някои автори, „стимулират приемането на схемите на Европейския съюз за качество на храните и които сигнализират за връзката между качеството на даден хранителен продукт и неговия географски произход“ [3: 3].

В тази връзка предмет на разглеждане в доклада са някои аспекти на продоволствената сигурност и необходимостта от активни разузнавателни мерки в тази насока.

Обект на изследване е връзката между продоволствения проблем, продоволствената сигурност и необходимостта от насочване на съвременното разузнаване към тази сфера.

Цел на разработката е да се посочи необходимостта от ориентация на съвременното разузнаване към компонентите на продоволствената сигурност и решаването на продоволствения проблем.

Материали и методи

За целите на изследването са използвани:

- литературни източници на български автори;
- анкетно проучване;
- обобщени резултати от проведено анкетно проучване на тема „Продоволствената сигурност в контекста на съвременното разузнаване“.

Резултати и обсъждане

Смекчаването и решаването на продоволствения проблем в Република България, освен че е предмет на аграрната политика в национален и регионален мащаб, би трябвало да е едно от основните направления в съвременното разузнаване.

За целите на доклада, както вече бе посочено, са използвани резултати от проведено анкетно проучване на тема „Продоволствената сигурност в контекста на съвременното разузнаване“.

Анкетното проучване се базира на обобщени резултати от анкетиране на принципа „лице в лице“, проведено на терен.

Анкетното проучване е осъществено в Югозападния район за планиране със земеделски производители.

Анкетирани са 102 души пълнолетни граждани, живеещи в съответните населени места.

Анкетата се състои от два раздела:

Първи раздел: Профил на респондента, и Втори раздел: Специализирани въпроси, съотносими към темата.

Обобщените резултати са представени по-долу, както следва по раздели, а именно:

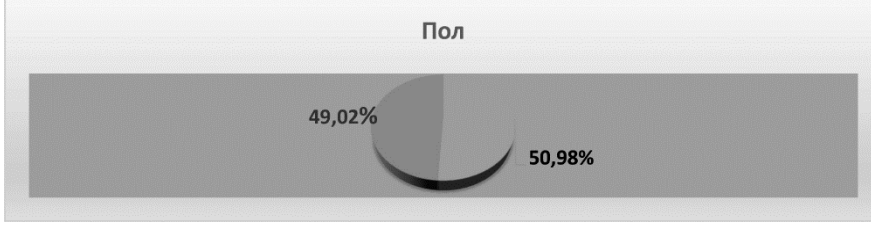
I раздел: Профил на респондента

1. Общ брой анкетирани – 102 души – 100 %

Фигура 1.

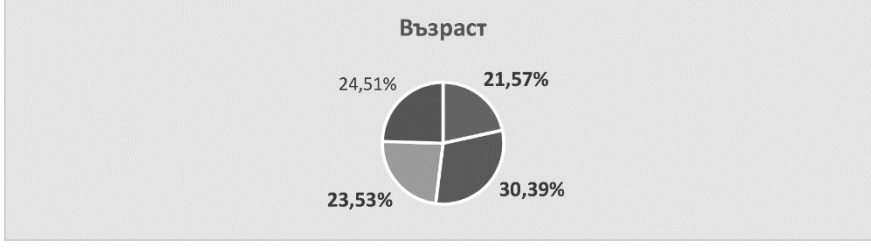
2. Пол:
а) мъже – 50 души, или 49,02 %
б) жени – 52 души, или 50,98 %

Фигура 2.



3. Възраст:
а) 18 – 30 години – 22 души, или 21,57 %
б) 31 – 40 години – 31 души, или 30,39 %
в) 41 – 50 години – 24 души, или 23,53 %
г) над 50 години – 25 души, или 24,51 %

Фигура 3.

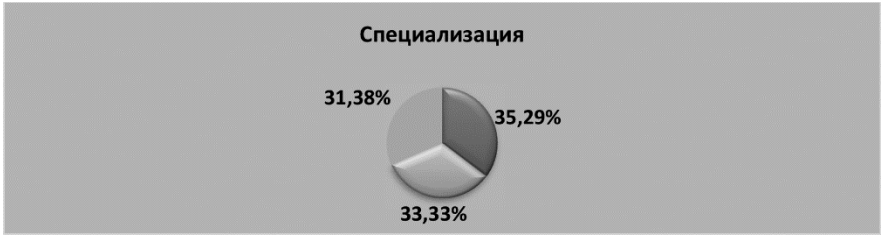


4. Стаж като земеделски производител:
а) 5 години – 13 души, или 12,75 %
б) 10 години – 24 души, или 23,53 %
в) 15 години – 31 души, или 30,39 %
г) над 15 години – 34 души, или 33,34 %

Фигура 4.

5. Специализация:
а) растениевъдство – 36 души, или 35,29 %
б) животновъдство – 34 души, или 33,33 %
в) и двете – 32 души, или 31,38 %

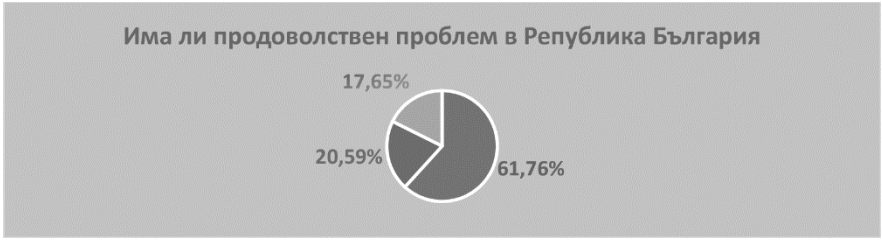
Фигура 5.



II раздел: Специализирани въпроси

1. Въпрос: Има ли продоволствен проблем в Република България?
а) да – 63 души, или 61,76 %
б) не – 21 души, или 20,59 %
в) донякъде – 18 души, или 17,65 %

Фигура 6.



2. Въпрос: Ако отговорът на предходния въпрос е „а“ или „в“, този проблем е свързан със (възможен е повече от един отговор)…?

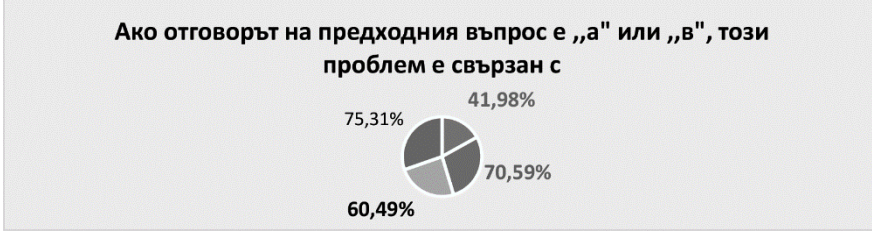
а) недостиг на някои земеделски продукти – 34 души, или 41,98 %

б) високи цени на земеделските продукти – 72 души, или 70,59 %

в) приоритетен внос на земеделски продукти – 49 души, или 60,49 %

г) неудовлетворително качество – 61 души, или 75,31 %

Фигура 7.

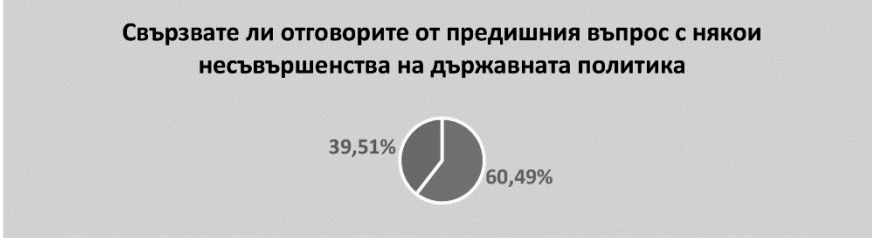


3. Въпрос: Свързвате ли отговорите на предишния въпрос с някои несъвършенства на държавната земеделска политика?

а) да – 49 души, или 60,49 %

б) донякъде – 32 души, или 39,51 %

Фигура 8.



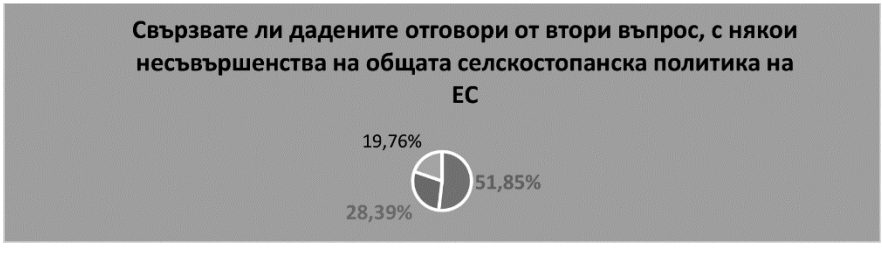
4. Въпрос: Свързвате ли дадените отговори на втори въпрос с някои несъвършенства на общата селскостопанска политика на ЕС?

а) да – 42 души, или 51,85 %

б) не – 23 души, или 28,39 %

в) донякъде – 16 души, или 19,76 %

Фигура 9.



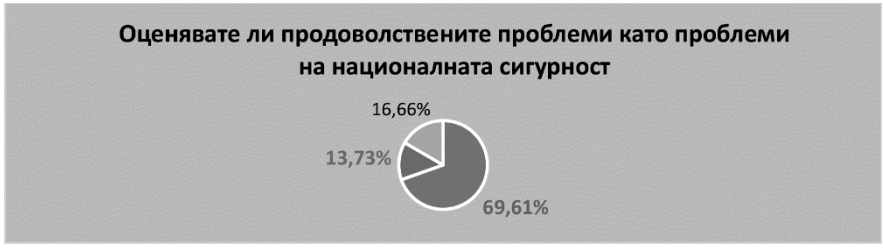
5. Въпрос: Оценявате ли продоволствените проблеми като проблеми на националната сигурност?

а) да – 71 души, или 69,61 %

б) не – 14 души, или 13,73 %

в) донякъде – 17 души, или 16,66 %

Фигура 10.

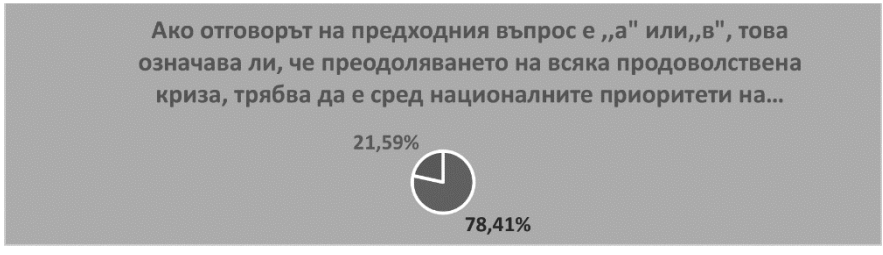


6. Въпрос: Ако отговорът на предходния въпрос е „а“ или „в“, това означава ли, че преодоляването на всяка продоволствена криза трябва да е сред националните приоритети на сигурността?

а) да – 69 души, или 78,41 %

б) не – 19 души, или 21,59 %

Фигура 11.



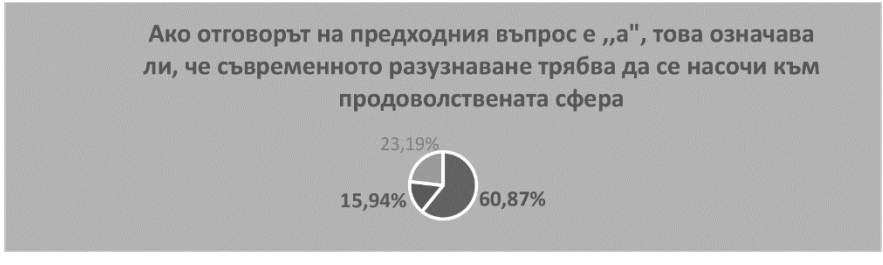
7. Въпрос: Ако отговорът на предходния въпрос е „а“, това означава ли, че съвременното разузнаване трябва да се насочи към продоволствената сфера?

а) да – 42 души, или 60,87 %

б) не – 11 души, или 15,94 %

в) донякъде – 16 души, или 23,19 %

Фигура 12.



Изводи

Показаните в изложението обобщени резултати от Раздел II на анкетното проучване дават основание за оформяне на следните изводи:

1. Основна част от анкетираните земеделски производители – 61,76 %, потвърждават наличието на продоволствен проблем в Република България.

2. Продоволственият проблем в Република България се свързва от по-голяма част от анкетираните с високи цени на земеделските продукти – 70,59 % от анкетираните, като на второ място се поставя неудовлетворителното качество на земеделските продукти – 75,31 %.

3. Наличието на тези нюанси на продоволствения проблем и продоволствената сигурност, в т.ч. недостигът на някои земеделски продукти и приоритетният внос на земеделски продукти, се свързват от 60,49 % от анкетираните с някои несъвършенства на държавната земеделска политика.

4. 51,85 % от анкетираните свързват характеристиките на продоволствения проблем, респективно на продоволствената сигурност, и с общата селскостопанска политика на Европейския съюз.

5. В тази връзка 69,61 % от анкетираните твърдо оценяват продоволствените проблеми именно като проблеми на националната сигурност, а 78,41 % смятат, че преодоляването на всяка продоволствена криза трябва да е сред националните приоритети на сигурността.

6. В този смисъл 60,87 % от анкетираните приемат, че съвременното разузнаване трябва да се насочи и към продоволствената сфера.

Литература

1. **Агростатистика.** Сборник, № 418, 2022 г. София: Министерство на земеделието и храните, 2022. ISBN 978- 619-90180-4-0. [онлайн]. *www.mzh.government.bg.*
2. **Давидова,** А. (2018). Храна има в изобилие – грешката е в разпределението. – В: *Фермер,* 7.04.2018 г. [онлайн]. *www.bgfermer.bg.*
3. **Марков,** Цв. (2025). Традиционните български храни за повишаване устойчивостта на местната икономика. – В: *Управленски* и екологични аспекти за повишаване устойчивостта при регионалното развитие на селските територии в България. Колективна монография. Свищов: Д. А. Ценов, 2025, с. 81. ISBN 978 954-23-2542-0.
4. **Николова,** М. (2025). Биологичното земеделие като фактор и необходимост за диверсификация. – В: *Управленски* и екологични аспекти за повишаване устойчивостта при регионалното развитие на селските територии в България. Колективна монография. Свищов: Д. А. Ценов, 2025, с. 106. ISBN 978 954-23-2542-0.

СИГУРНОСТ И ВОДНИ РЕСУРСИ – НЕОБХОДИМОСТ В РАЗУЗНАВАТЕЛНАТА СФЕРА (НА ПРИМЕРА НА АНКЕТНО ПРОУЧВАНЕ)

проф. д-р Гена Велковска
Висше училище по сигурност и икономика – Пловдив

SECURITY AND WATER RESOURCES – A NECESSITY IN THE INTELLIGENCE SPHERE (ON THE EXAMPLE OF A SURVEY)

Prof. Gena Velkovska, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Водните ресурси обуславят както задоволяване на потребностите на населението, така и удовлетворяване на технологичните нужди на редица отрасли на икономиката, сред които един от основните консуматори е аграрният сектор. В нормативен план питейната вода е квалифицирана като стратегически ресурс, но това се отнася за всички елементи от водния баланс на страната. Управлението на водните ресурси, тяхното опазване и поддържане от гледна точка на тяхната значимост е проблем и на националната сигурност. В тази връзка трябва да се подчертае, че управлението на водните ресурси може да бъде успешно подпомагано от различни разузнавателни способи.*

Ключови думи: *води; водни ресурси; сигурност; разузнавателни способи; воден баланс*

Abstract: *Water resources determine both the satisfaction of the needs of the population and the satisfaction of the technological needs of a number of sectors of the economy, among which one of the main consumers is the agricultural sector. In regulatory terms, drinking water is qualified as a strategic resource, but this applies to all elements of the country's water balance. The management of water resources, their protection and maintenance, from the point of view of their importance, is also a problem of national security. In this regard, it should be emphasized that the management of water resources can be successfully supported by various intelligence methods.*

Key words: *waters; water resources; security; intelligence methods; water balance*

Въведение

Според нормата на чл. 3 от Закона за водите [2: 1] води на територията на страната са:

- повърхностните води;
- подземните, включително минералните води;
- вътрешните морски води и териториалното море;
- водите на река Дунав, река Резовска и река Тимок в рамките на държавната граница на Република България.

Една от основните функции на водите е да бъдат жизненоважен ресурс, обслужващ населението, аграрния сектор, енергийния сектор и други отрасли и дейности без вреда за обществените интереси и без да се нарушава технологичното единство на водностопанската система.

Според нормата на чл. 3а, ал. 1 от Закона за водите [5: 2] пресните води на територията на Република България са национални стратегически ресурси. В тази връзка те имат пряко отношение към националната сигурност независимо от собствеността – собственост на държавата, собственост на общините, собственост на физически и юридически лица.

В качеството им на фактор за национална сигурност водните ресурси се ползват със закрила, доколкото с упражняването на собственост върху тях не се уврежда целостта и единството на хидроложкия цикъл и на природната водна система по смисъла на чл. 7, т. 3 от Закона за водите.

Климатичните промени през последните години повлияха сериозно върху водните ресурси и хидрогеоложката система като цяло. Водната сигурност изцяло попада в кризисни ситуации поради няколко причини. Освен посочения климатичен фактор, важна роля имат нерационалното управление на водните ресурси, неикономичният подход и нерационалното използване.

В някои райони на страната ситуацията с водните ресурси е критична поради тяхната оскъдност.

Според някои автори при изследване на относителния дял на територията, заета от води и водни обекти по статистически райони за периода 2021 – 2023 г., Северозападният район има най-висок дял територия, заета от водни обекти – 2,36 %, докато Югозападният е с относителен дял 1,14 % [3: 2].

По отношение на отпадъчните води (образувани и отведени) по статистически райони за периода 2018 – 2022 г. данните показват нарастване на отпадъчни води в Югозападния район и съответно намаляване в Северния Централен район и в Северозападния район [4: 3].

Сериозен проблем в поддържането на параметрите на водната сигурност е недоброто състояние на хидромелиоративната инфраструктура в Република България, касаещ и сигурността в аграрния сектор [1: 3].

Предмет на разглеждане в доклада са някои аспекти на сигурността, касаеща водните ресурси, респективно водния сектор и неговото обслужване от разузнавателната сфера.

Обект на разглеждане са актуалните проблеми с водните ресурси, произтичащи от конкретни фактори от законодателно, обективно и субективно естество, с които е застрашена и нарушена националната сигурност.

Цел на изследването е да се обоснове необходимостта от превръщането на водната сигурност в направление на разузнавателната сфера от гледна точка на водния сектор като стратегически за страната.

Материали и методи

За целите на изследването са използвани:

- литературни източници на български автори;
- нормативни източници (акценти от действащата нормативна уредба);
- аналитичен инструментариум (нормативен и аналитичен методологичен апарат) и анкетно проучване;
- обобщени резултати от проведено анкетно проучване на тема „Сигурност и водни ресурси – необходимост в разузнавателната сфера“.

Резултати и обсъждане

Министерският съвет на Република България по смисъла на чл. 10, ал. 2 от Закона за водите приема Стратегия за развитие и управление на водоснабдяването и канализацията в Република България за период, не по-малък от 10 години.

Целесъобразно и наложително е тази Стратегия да бъде обвързана със Стратегията за национална сигурност като цяло и да бъде обект също така на разузнаването.

За целите на доклада, както вече бе посочено, са използвани резултати от проведено анкетно проучване на тема „Сигурност и водни ресурси – необходимост в разузнавателната сфера“.

Анкетното проучване е направено през м. март 2025 г. по метода „лице в лице“ и обхваща извадка от 68 души пълнолетни български граждани на територията на гр. София.

Анкетата се състои от два раздела:

Първи раздел: Профил на респондента, и Втори раздел: Специализирани въпроси, съотносими към темата на изследването.

Обобщените резултати са представени по-долу, както следва, по раздели, а именно:

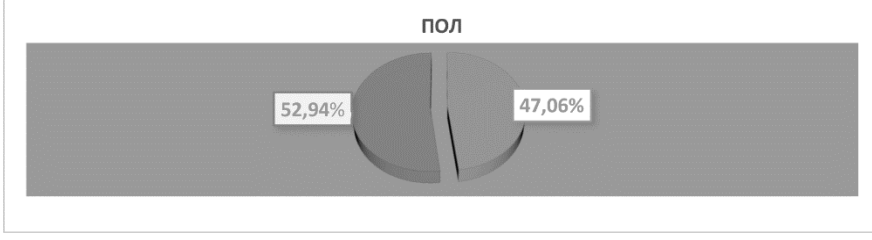
I раздел: Профил на респондента

1. Общ брой анкетирани – 68 души – 100 %

Фигура 1.

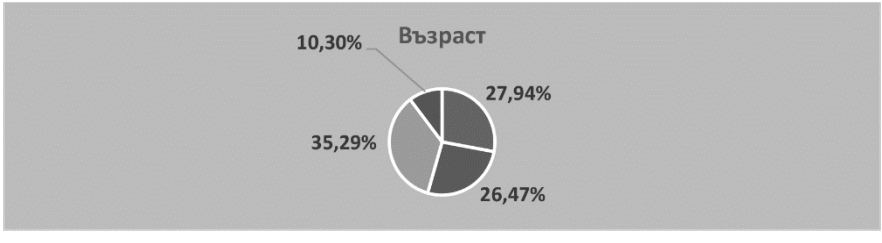
2. Пол:
а) мъже – 36 души, или 52,94 %
б) жени – 32 души, или 47,06 %

Фигура 2.



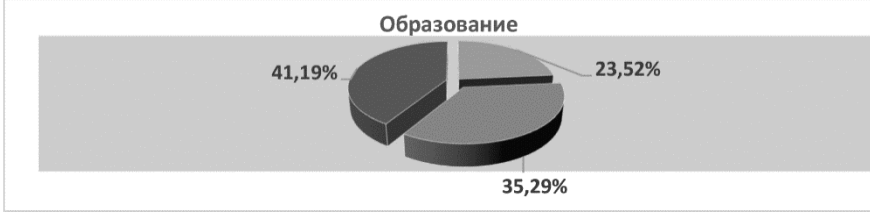
3. Възраст:
а) 18 – 25 години – 24 души, или 35,29 %
б) 26 – 40 години – 18 души, или 26,47 %
в) 41 – 55 години – 19 души, или 27,94 %
г) над 55 години – 7 души, или 10,30 %

Фигура 3.



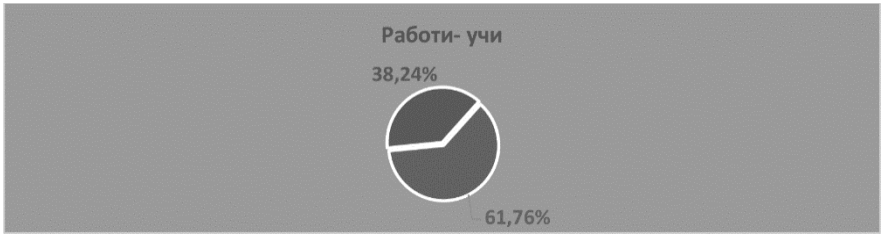
4. Образование:
а) средно – 16 души, или 23,52 %
б) висше – 24 души, или 35,29 %
в) друго – 28 души, или 41,19 %

Фигура 4.



5. Работи, учи:
а) работи – 42 души, или 61,76 %
б) учи – 26 души, или 38,24 %

Фигура 5.



II. Специализирани въпроси

1. Въпрос: Има ли проблем с водните ресурси в България?
а) да – 38 души, или 55,88 %
б) не – 13 души, или 19,12 %
в) до известна степен – 17 души, или 25,00 %

Фигура 6.

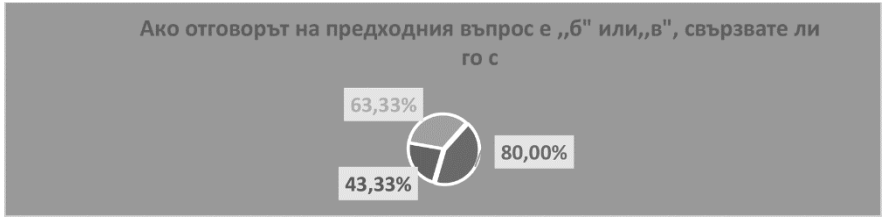
2. Въпрос: Ако отговорът на предходния въпрос е „б“ или „в“, свързвате ли го със (възможен е повече от един отговор)…?

а) климатични промени – 19 души, или 63,33 %

б) държавна политика – 13 души, или 43,33 %

в) разхищаване на водния ресурс от страна на субективния фактор – 24 души, или 80,00 %

Фигура 7.



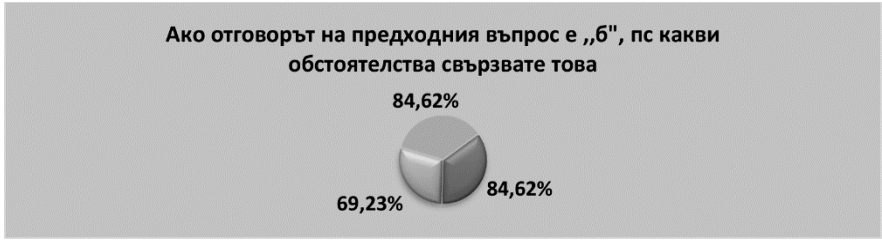
3. Въпрос: Ако отговорът на предходния въпрос е „б“, с какви обстоятелства свързвате това (възможен е повече от един отговор)?

а) остаряла ВиК инфраструктура – 11 души, или 84,62 %

б) напоителни системи в критично състояние – 9 души, или 69,23 %

в) непоставяне на водните ресурси като приоритет в държавната политика – 13 души, или 84,62 %

Фигура 8.



4. Въпрос: Концесионната политика на общините по отношение на минералните извори подпомага ли регионалното развитие?

а) да – 22 души, или 32,35 %

б) не – 33 души, или 48,53 %

в) до известна степен – 13 души, или 19,12 %

Фигура 9.

5. Въпрос: Ако отговорът на предходния въпрос е „б“ или „в“, причината за това е…?

а) политиката на самите фирми и частни лица – 28 души, или 60,87 %

б) липсата на контрол от страна на общините – 18 души, или 39,13 %

Фигура 10.

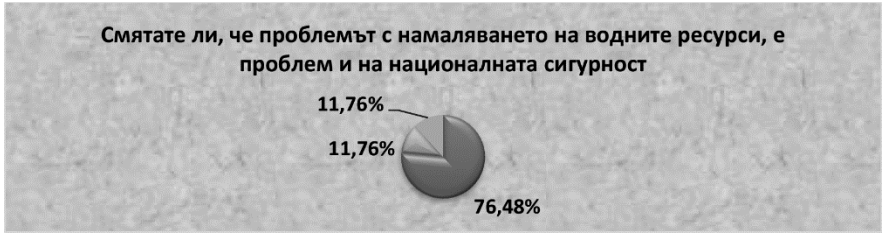
6. Въпрос: Смятате ли, че проблемът с намаляването на водните ресурси е проблем и на националната сигурност?

а) да – 52 души, или 76,48 %

б) не – 8 души, или 11,76 %

в) до известна степен – 8 души, или 11,76 %

Фигура 11.

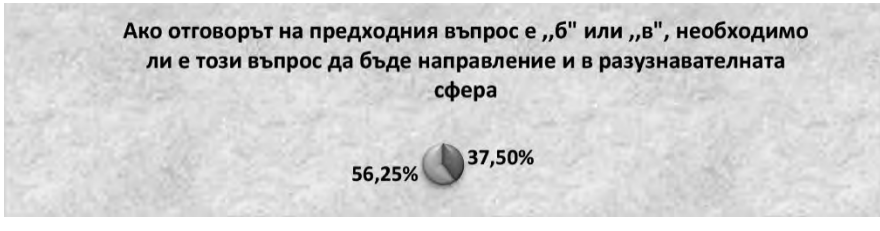


7. Въпрос: Ако отговорът на предходния въпрос е „б“ или „в“, необходимо ли е този въпрос да бъде направление и в разузнавателната сфера (възможен е повече от един отговор)…?

а) да – 14 души, или 87,50 %

б) до известна степен – 9 души, или 56,25 %

Фигура 12.



Изводи

Обобщените резултати от проведеното анкетиране налагат следните изводи:

1. По-голяма част от анкетираните – 55,88 %, констатират, че България има проблем с водните ресурси, а 19,12 % смятат, че такъв проблем няма.

2. Негативният отговор на част от анкетираните се свързва главно с разхищаване на водния ресурс от страна на субективния фактор – 80,00 %, с климатичните промени – 63,33 %, и с държавната политика в сектора – 43,33 %.

3. Държавната политика в сектора от гледна точка на нейната нерационалност се свързва основно с обстоятелството, че водните ресурси не се поставят като приоритет в държавната политика.

4. По отношение на концесиите и концесионната политика на общините, касаеща минералните извори, 48,53 % отговарят, че тази политика не подпомага регионалното развитие, като причината за това е според по-голяма част от анкетираните – 60,87 %, политиката на самите фирми и частни лица концесионери.

5. 76,48 % от анкетираните смятат, че проблемът с намаляването на водните ресурси е проблем на националната сигурност, и в тази връзка подкрепят констатацията за необходимостта този въпрос да бъде направление в разузнавателната сфера – 87,05 %.

Литература

1. **Велковски,** В. (2024). Хидромелиоративната инфраструктура в Република България – специфики, проблеми и перспективи. – В: *Научни* трудове на Аграрен университет – Пловдив, том LXVI, кн. 1, 2024 г. (Научна конференция на тема „Ролята на фамилния бизнес за устойчиво развитие“, Аграрен университет – Пловдив, 2024 г., с. 95. ISSN (Print) 1312-6318. ISSN (Online) 2367-5845.)
2. **Закон** за водите. В сила от 28.01.2000 г. Обн. *ДВ,* бр. 67 от 27.07.1999 г.; изм. *ДВ,* бр. 81 от 6.10.2000 г.; изм. *ДВ,* бр. 79 от 17.09.2024 г.
3. **Стоянова,** З. (2025). Състояние на природните ресурси по статистически райони. – В: *Управленски* и екологични аспекти за повишаване устойчивостта при регионалното развитие на селските територии в България. Колективна монография. Свищов: Д. А. Ценов, 2025, с. 125. ISBN 978 954-23-2542-0.
4. **Стоянова,** З. (2025). Анализ на въздействието върху природните ресурси по статистически райони. – В: *Управленски* и екологични аспекти за повишаване устойчивостта при регионалното развитие на селските територии в България. Колективна монография. Свищов: Д. А. Ценов, 2025, с. 129. ISBN 978 954-23-2542-0.
5. *www.lex.bg.*

TRANSNATIONAL ORGANIZED CRIME IN RELATION TO THE RISK OF MONEY LAUNDERING AND TERRORIST FINANCING AS A FRIGHTENING FACTOR FOR SECURITY

Assoc. Prof. Aleksandra Jovanović, PhD
Faculty of Business Economics and Entrepreneurship – Belgrade, Serbia
Dragutin Franculović, PhD student
Higher School of Security and Economics – Plovdiv, Bulgaria
Nikola Jovanović, MA student
Faculty of Mechanical Engineering, University of Niš, Serbia

ТРАНСНАЦИОНАЛНАТА ОРГАНИЗИРАНА ПРЕСТЪПНОСТ ПО ОТНОШЕНИЕ НА РИСКА ОТ ПРАНЕ НА ПАРИ И ФИНАНСИРАНЕ НА ТЕРОРИЗМА КАТО ЗАПЛАШВАЩИ ФАКТОРИ ЗА СИГУРНОСТТА

доц. д-р Александра Йованович
Факултет по бизнес икономика и предприемачество – Белград, Сърбия
докторант Драгутин Францулович
Висше училище по сигурност и икономика – Пловдив, България
студент Никола Йованович
Факултет по машинно инженерство на Университета в Ниш, Сърбия

Abstract: *Transnational organized crime represents one of the most dangerous unconventional threats to a large number of states in the modern world. Transnational organized crime, a negative social phenomenon, manifests constant dynamism, and it is necessary to bring it under as much control as possible, especially from the aspect of its manifestation and threatening effect on security, to eliminate or mitigate its harmful phenomenon through timely, preventive, and repressive action.*
Key words: *transnational organized crime; money laundering; terrorism, security; risk*

Резюме: *Транснационалната организирана престъпност представлява една от най-опасните неконвенционални заплахи за голям брой държави в съвременния свят. Транснационалната организирана престъпност е негативно социално явление, което проявява постоянна динамика и е необходимо тя да бъде поставена под възможно най-голям контрол, особено от гледна точка на нейното проявление и заплашително въздействие върху сигурността, за да се елиминира или смекчи нейното вредно явление чрез навременни, превантивни и репресивни действия.*
Ключови думи: *транснационална организирана престъпност; пране на пари; тероризъм; сигурност; риск*

Introduction

Transnational crime, a global phenomenon, seeks to develop and survive in the international arena, finding models of action and opportunities for self-protection. In this direction, this criminality tends to enjoy certain privileges by using criminal connections with the state, its political structure, and its organs. This relationship is based on the use of corruption, use of blackmail, force, coercion or intimidation, and other illegal means. Organized criminal groups are often associated with executive authorities in a state that uses its own „privilege of power“. Striving to survive and develop further, transnational organized crime finds appropriate forms of self-protection and enjoyment of certain privileges through the use of force, intimidation, and the establishment of criminal ties with the state, its organs,

political structures, and strong financial and economic systems. Transnational organized crime tries to take advantage of all the favorable conditions for the realization of the plans of organized criminal groups, thus enabling its survival. The appetites of organized criminal groups are greater than that, they are reflected in the expansion and connection of these groups and their activities, but also the expansion of criminal activity The expansion of the criminal activity of organized groups occurs in infiltrating into new spheres of action and profit, greater connection of groups, expansion of the area of action, and use of areas of social, economic, and political life that will favor the strengthening of their organizational ability and their interests and goals. All of these are the reasons for the necessity of assessing the risk of money laundering and terrorist financing as a factor threatening security, which includes an assessment of threats, vulnerabilities, and consequences for the system (FATF) and the security of the state and society.

Objective and methods

The scientific goal of the article is a scientific description and explanation of transnational organized crime and the risks that represent a factor in the impact of money laundering and terrorist financing as segments of this crime on national security.

The practical goal of the article is to point out the shortcomings at the strategic and operational level within the Republic of Serbia with the ultimate goal presented in the conclusion, which presents concrete proposals for reducing the risk to national security from factors that affect it – money laundering and terrorist financing.

Methods applied in the article are: content analysis, statistical method, and legal dogmatic method.

Transnational organized crime

The term transnational organized crime did not have, nor has it been given, a real meaning, but is a criminological term under which we can subsume many things that are defined differently and differently in the criminal laws of countries, but with the common attribute of a phenomenon that exceeds the jurisdiction of any given state (Zirojević, Đukanović, Gajić 2013, p. 49), which indicates its international character. Transnational crime was defined for the first time at the UN Branch for Crime Prevention and Criminal Justice, which refers to the preparation of the 5th UN Congress on the Prevention of Crime and the Treatment of Offenders held in Geneva in 1975. The name of this type of crime represents a criminological term that denotes criminal activities that have an international – transnational character. Transnational organized crime can be defined as organized crime coordinated across national borders, which includes groups or markets of individuals working in more than one country to plan and carry out illegal actions. According to Bossard, the former Secretary General of Interpol, the international character is reflected in the fact that the offender „crossed“ at least one border when committing an illegal act and that the nature of the act, its consequences and the transnational nature of the activity are determined by the perpetrator himself (Bosard 1990). Bossard believes that a crime acquires an international character only if the undertaken activities are incriminated in the laws of a specific country. For this reason, transnational crime should contain the following elements:

- crossing the state border by individuals (criminals or victims), things or criminal intent (abuses in the field of electronic payments with accounts in different countries), and
- international recognition that it is a crime.

The same author points out that the aforementioned crimes provided that they are considered crimes in at least two countries, belong to transnational organized crime, provided that criminal gangs meet the following conditions: permanence, excellent structure, strict hierarchy, and secrecy (Joksić & Božović 2013, p. 44).

We see transnationality in the designation of organized crime by the United Nations, which defines an organized criminal group as a group of three or more persons who act in concert by committing criminal acts for the purpose of obtaining financial or other material benefits (UN Convention, p. 20). The United Nations Convention against Transnational Organized Crime, adopted by United Nations General Assembly Resolution 55/25 of November 15, 2000, is a basic instrument of international character in the fight against transnational organized crime. Transnational organized crime in the Convention is conditionally classified into four separate entities: criminalization of participation in an organized criminal group, criminalization of „laundering" of profits obtained by committing criminal acts, criminalization of corruption and criminalization of obstruction of justice.

The positive legislation of the Republic of Serbia foresees the possible transnationality of organized crime based on the planned activity of the criminal collective in international frameworks.

Organized crime, illegal activity, largely depends on the „criminal economic market" or „illegal market" and the will of state entities to suppress them. The activities of organized crime are numerous and diverse, they manifest themselves in different forms and intensities, and their forms of action are effectively adapted to existing current social movements and events (Kržalić et al. 2014, p. 12). Organized crime has some transnational characteristics. Transnational organized crime manifests itself through various forms of criminal activity. The emergence of new forms of crime at the global, regional and local level should be seen in the light of the dynamics of transnational connection of criminal groups, but, of course, bearing in mind that traditional criminal organizations and transnational organized criminal groups are not necessarily the same phenomenon (Arsovska, Allum 2014). In this manifestation, he is looking for suitable bases for his survival, expansion and the greatest possible spread in the international space. The drive towards globalization, unification of the world market of capital and technology, and the transition of underdeveloped countries contribute to the development of transnational crime, organized illegal activity. The transnational model of the criminal market is represented by organized criminal collectivities, homogeneous (ethnic and/or multi-ethnic) and organized on the territory of one or more countries, which also carrys out transnational activities. Members of organized crime act for the illegal acquisition of property benefits, which they translate into legal flows, leaving the possibility that they can turn their own interest of enrichment into political interest, which they achieve by financing terrorist activities. p. Such a case is money laundering for the purpose of financing terrorism. In this way, transnational organized crime poses a threat to national security. Often corruption, force or threats are used to achieve the goal of profiteering, further for the purpose of preserving immunity from the application of law (Albanese 2000, p. 412). What is an additional worrisome circumstance is „the establishment of a connection between the heads of criminal organizations and individuals from the structure of state authorities" (Bošković 2003, p. 7). The model of operation of transnational organized crime based on corruption represents a more effective way of protecting and promoting criminal interests, because by influencing public authorities, directly or indirectly, the effects of crime suppression policies are prevented or reduced (the organizational, technological, spatial and temporal complexity of transnational organized crime, among other things, legitimizes it as a threatening factor that seeks to ensure its survival and protection through the use of force or intimidation, preferably using established positions in state institutions (Lakićević 2018, pp. 105-106).

A significant factor endangering security – transnational organized crime leads to problems and negativity in society through implementation; illegal production and drug trade, use of cyber space and computer terrorism, illegal transfer of weapons, endangering the environment, racketeering and money laundering (Gunaratna 2001, 46). According to the Global Organized Crime Index published for 2020, Serbia ranked 33rd with 6.21 index points, slightly below Russia, and is the first European country among 193 UN member states.

Transnational organized crime is not equally present in all countries. The degree of its threat is determined by the intertwining of numerous economic, political, social, and cultural facts, legislative solutions, models of the fight against it, and the effectiveness of preventive actions in the direction of its suppression.

Significant sources of income of transnational organized crime are achieved through: human trafficking, prostitution, arms and ammunition trade, drug trade, illegal sale of human organs, illegal sale of children, corruption, terrorism, and money laundering.

Risk of money laundering

One of the hallmarks of transnational organized crime is the laundering of money obtained through criminal activity through various transactions (financial, economic, etc.) and the introduction of „dirty money" into legal flows. When the money earned by crime is introduced into legal flows, it reaches the stage of integration, it is difficult to distinguish between permitted and illicit funds. As such, through the exercise of its „power" through legal and illegal channels, organized crime affects the economic and political spheres of social life. How money is laundered varies greatly depending on the level of expertise of the members of organized criminal groups themselves, as well as on the frequency and scope of criminal activity. Typologies and trends of money laundering have been repeated for many years. It is expected that the trend of money laundering will also be present in the future with the growth of international payment transactions. At the global level, in addition to numerous offshore companies, the existence of business entities called providers for money laundering, whose services are used by organized criminal groups.

This type of money laundering represents a high-risk area because it can relatively easily absorb large amounts of capital. In addition to this form, for money laundering and its legalization, the banking sector, the sector of games of chance, the sector of electronic money issuers, service providers connected with digital assets, and the capital market sector are used. The Criminal Code stipulates that the property that is the subject of the criminal offense of money laundering originates from criminal activity, unlike earlier determinations according to which it originates from a criminal offense. Acceptance of this more comprehensive description of the origin of illegally acquired property, which does not require the provision of more detailed information about the alleged criminal offense, in the current code facilitates criminal prosecution and proof.

According to the European assessment of the threat of financial and economic crime in 2023, financial crimes, especially money laundering, undermine our society not only by infiltrating the legal economy, but also by encouraging the growth of a parallel underground society, made up of individuals who increasingly rely on organized crime for their economic support and livelihood. Because of their intrusive and explosive nature, financial and economic crimes are among the most challenging criminal activities to investigate and combat. The criminal image consists of different actors who cooperate with each other. The explosive nature of this crime, the number of actors, mutual cooperation and adaptation to technological changes make criminal operations more complex and intricate.

States, including the Republic of Serbia, assess the risk of money laundering and the assessment of the financing of terrorism. The goal of risk assessments is to determine the areas and actions in the system of a country that carry a potentially higher or lower risk of money laundering and terrorist financing, so that the country can adequately respond to the identified risks with a series of measures and activities and, by the assessed risks, make adequate decisions on the allocation of resources, to invest more efforts and resources in high-risk areas. Identifying, assessing and understanding the risk of money laundering and terrorist financing represent an essential part of the implementation and development of the system for preventing money laundering and terrorist financing in the country. The mentioned risk assessments are also extremely important for the adequate implementation of regulations in the field of prevention of money laundering and financing of terrorism by the private sector. The national risk assessment is carried out by a working group formed by the Government of the Republic of Serbia. This random group is managed by the Public Prosecutor's Office, an organized criminal. Within that group, there are representatives of those liable (according to the Law on the Prevention of Money Laundering and Terrorism Financing) for risk assessment: the Directorate for the Prevention of Money Laundering, the Supreme Court, the Supreme Public Prosecutor's Office, the Public Prosecutor's Office for Organized Crime, the Securities Commission, the Security and Information Agency, the Ministry of the Interior, the Ministry of Justice, the Office of the Council for National Security and the Protection of Secret Data, and the National Bank of Serbia. The analysis of money laundering threats and national vulnerability to money laundering determined the comprehensive risk of money laundering: a) for the „medium“ period from 2013 to 2018, b) „low“ for the period from 2018 to 2020“.

It is necessary to point out predicate crimes that are classified as a high degree of threat for money laundering: tax crimes, abuse of office and unauthorized production and distribution of narcotic drugs. Acts of high-tech crime have an increasing stake. Based on the analysis of data from criminal proceedings and indictments in the Republic of Serbia presented in the Money Laundering Risk Assessment and Terrorism Financing Risk Assessment, it was determined:

- In the period from 2013 to 2017, 55.3% of defendants were prosecuted for self-laundering. Of the total number of persons prosecuted for the crime of money laundering, 24.61% were members of organized criminal groups. In the analyzed period, the most exposed to the threat of money laundering are the banking sector, the real estate sector, and the sector of organized games of chance.

- In the period from 2018 to 2020, 45.89% of defendants were prosecuted for self-laundering, and 30.30% were prosecuted for laundering money for another. 23.81% of the defendants were accused of money laundering without a predicate crime. The Prosecutor's Office for Organized Crime initiated proceedings against the defendants for the criminal offense of money laundering. The sectors most exposed to the risk of money laundering are the same as in the previous period.

Terrorist financing risk

The risk of financing terrorism in the period from 2013 to today is assessed as medium-low. This national assessment is based on an assessment of the threat of terrorism(Jovanović 2022, p. 138) and terrorist financing, where the threat of terrorist financing by terrorists and terrorist organizations is low, the threat of terrorist financing at the national level is medium-low, and the country's vulnerability to terrorist financing is low. The low rating is supported by the fact that no criminal prosecution was undertaken for acts of terrorist financing and related acts.

Despite this assessment of the risk of terrorism and its financing, threats to national security are possible: migrant movements and the possibility of the return of foreign terrorists. These threats are assessed as high considering that they are international and the Republic of Serbia can hardly influence them. The question arises: is migration an artificial creation? If this question is answered in the affirmative, then this type of migration certainly leads to a high risk of terrorism. A further question arises: who finances such migrations? This question is difficult to answer from a theoretical point of view. The assumptions should be reviewed at the national and international level by the appropriate structure and competent institution.

In order for the national security system to cope more successfully with terrorist aggression and the financing of terrorism, a comprehensive, legal, preventive, centralized, offensive and self-critical defense of national security is necessary in relation to challenges or threats (Jovanović 2019, p. 299).

Deficiencies at the strategic and operational level within the Republic of Serbia

Deficiencies at the strategic level present in the Republic of Serbia relate to:

- Absence of a special body at the state level to coordinate the activities of participants in the system for combating money laundering and terrorist financing.
- Absence of uniformity of data in the records of competent authorities.
- Failure to update the national assessment of the risk of money laundering on an annual basis, given that with the development of society and technology, as well as the model of execution of this act, it becomes more widespread.
- Raising doubts about the existence of a connection between the government=political structure and crime.

Disadvantages at the operational level:

- insufficient cooperation of participants in the system of fighting against this criminal behavior,
- insufficient international cooperation,
- insufficient number of parallel financial investigations,
- insufficient engagement of the Agency for the fight against corruption,
- insufficient action of the Public Prosecutor's Office of the Republic on official duty in the presence of suspicion of the commission of an illegal act of money laundering,
- insufficient use of the capacity for confiscation of property benefits acquired through criminal acts
- mild penal policy,
- privileges of „big“ institutions – taxpayers when paying taxes, in the form of tax reduction and payment in installments (which in a way represents „lawful action“),
- mild penal policy,
- absence of real ownership register and
- absence of ownership register in the country and abroad.

Although it is almost impossible to eradicate the activities of organized crime, it is necessary to have a national strategy, but also an international strategy, which will enable a more adequate approach to the emerging forms of organized crime, i.e. control of the emergence of new forms of organized crime and their development and effective realization of the concrete causes based on which organized crime is constantly progressing (Matijašević & Pavlović 2009, p. 64).

Conclusion

This inevitably leads to the need for preventive action and suppression of transnational organized crime. The fight against transnational organized crime requires the efforts of state institutions in cooperation with civil society, non-governmental organizations, and police cooperation, which can develop into police partnerships. This struggle must be accompanied by the construction and development of interstate cooperation and the undertaking of concrete actions aimed at suppressing it. The process of fighting against organized crime, which is otherwise difficult to eradicate, continues continuously. It is desirable to reduce it to certain frameworks that allow it to be brought under control. This struggle is addressed by the Convention, which, in addition to recommending the seizure and confiscation of property acquired through the commission of criminal acts by organized criminal groups. In the fight against the suppression of this crime, international cooperation on a preventive and repressive level is also important, with the application of national legislation and international acts and respect for Jewish rights. Transnational organized crime as a threat to security must be viewed in connection with economic trends and with consideration of the factors that affect security: diversity of states, globalization, the transition of states, social order, and economic, cultural, and sociological levels. Economic aid in resolving the stability of a state as a preventive instrument for preventing internal conflicts of state collapse and non-implementation of destructive ways of leading external, and internal policy implies humanitarian and development aid (Jovanović 2022). Actions to combat transnational crime should be accompanied by strengthening the resilience of logistics hubs (EUROPOL), breaking criminal networks, increasing prevention efforts strengthening cooperation with international partners, and adopting measures to prevent organized crime.

Proposal of measures to be applied in the fight against transnational organized crime and money laundering:

- develop an approach to the involvement of the entire Government in the fight against transnational organized crime and the transparency of the results of the fight,
- strengthen the fight against organized criminal groups through professional bodies,
- improve internal international cooperation through the signing of agreements,
- improve the legal framework that is applied in investigations and prosecutions of perpetrators of crimes in the field of transnational organized crime with international and EU standards,
- improve institutional capacities and strengthen professional development for the implementation of measures to combat transnational organized crime,
- to form a permanent coordination body at the national level,
- strengthen interstate cooperation,
- weaken the links between transnational organized crime and corruption
- eliminate deficiencies at the strategic and operational levels.

Literature

1. **Bajagić,** M. (2009). Inostrana iskustva u razvoju teorijskog i organizacionog koncepta kontraobaveštajne aktivnosti. – In: *Bezbednost,* Beograd, pp. 370-385.
2. **Banović,** B. (2016). Organizovani kriminal kao aktuelna bezbednosna pretnja. – In: *Internationals* problems, MP, Vol. LXVIII, br. 2-3, str. 172-192. DOI:10.2298/MEDJP1603172B.
3. **Counterintelligence** Operations. (1993). Headquarters Department of the Army US, Washington DC, No. 30-17, п. 24.
4. **Đorđević,** O. (1986). Leksikon bezbednosti. – In: *Partizanska* knjiga, Beograd, p. 183.
5. **Dragišić,** Z. (2009). Sistem nacionalne bezbednosti: Pokušaj definisanja pojma. – In: *Vojno* delo, 3/2009, pp. 162-176.

6. **Đurdjević,** D., M. Stevanović. (2016). Internet trolovanje kao metod ofanzivnog obaveštajnog delovanja u kiberprostoru. – In: *Žurnal* za kriminalistiku i pravo, pp. 13-31. DOI: 10.5937/nabepo22-12060.
7. **Đurđević,** Ž., M. Stevanović. (2016). Obrazovanje za nacionalnu bezbednost. Beograd: Akademska misao.
8. **Harfield,** C. Pro-activity, Partnership and Prevention. – In: *The* Police Journal, 2000, br. 2, str. 109.
9. **Izveštaj** o napretku Srbije za 2012. godinu. Evropska komisija, Brisel, 10.10.2012, SEC (2012) 333, str. 75.
10. **Jovanović,** A. (2019). Organizing a european security strategy and cyber security in the Republic of Serbia as a response to cyber terrorism. – In: *Međunarodna* naučna konferenija „Savremeni trendovi u razvoju saobraćaja i bezbednosti regiona jugoistočne Evrope", „Konstantin Veliki", Niš, pp. 205-218.
11. **Jovanović,** A. (2022). Međunarodno krivično parvo. Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd.
12. **Jovanović,** A. (2024). Krivičnoprocesno parvo. Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, pp. 166-212.
13. **Korać,** S. (2011). Organizovani criminal kao bezbednosna pretnja Evropskoj uniji. – In: *Društveni* aspekti organizovanog kriminala, Beograd, pp. 410-450.
14. **Lakićević,** M. (2022). Kontraobaveštajna delatnost u funkciji suzbijanja organizovanog kriminala. – In: *Nacionalni* interes, god. XVII, vol. 41, br. 1/2022, pp. 123-145. DOI:10.22182/ni.4312022.6. *https: doi.org//10.22182/ni.4312022.6.*
15. **Lončar,** M., D. Marić. (2022). Ekonomska obaveštajnost u savremenim ekonomsko-bezbedonosnim okolnostima. – In: *Ekonomija,* teorija i praksa, god. XV, br. 2, pp. 107-126. DOI:10.5937etp2002107L.
16. **Marinković,** D. (2006). Kriminalistička strategija suzbijanja organizovanog kriminaliteta – osnovni konstitutivni elementi. – In: *Zbornik* radova: Sprečavanje i suzbijanje savremenih oblika kriminaliteta. Kriminalističko policijska akademija, pp. 13-36.
17. **Merriam** Webster dictionary. [online]. [available 20.06.2008]. *http://www.merriam-webster.com/dictionary/counterintelligence.*
18. **Mijalkovski,** M. (2009). Obaveštajne i bezbednosne službe. – In: *Službeni* glasnik, Beograd, pp. 32-33.
19. **Mijalković,** S. (2010). O nedržavnom sektoru nacionalnog sistema bezbednosti – inostrana i domaća iskustva. – In: *Strani* pravni život, 2/2010, pp. 251-269.
20. **Mijalković,** S. (2010). Obaveštajne strukture terorističkih kriminalnih organizacija. – In: *Nauka,* bezbednost i policija, no. 15.
21. **Mijalković,** S. (2011). Obaveštajno-bezbednosne službe i nacionalna bezbednost. – In: *Bezbednost,* br. 1, Kriminalističko-policijska akademija, Beograd, pp. 74-92.
22. **Mijalković,** S. (2010). O nedržavnom sektoru nacionalnog sistema bezbednosti – inostrana i domaća iskustva. – In: *Strani* pravni život, 2/2010, pp. 251-269.
23. **Schell,** O. (2007). Follies of Orthodoxy. – In: *What* Orwell Didn't Know: Propaganda and the New Face of American Politics. A. Szántó. (Ed.). New York: Public Affairs.
24. **Shorer-Zeltser,** M., G. M. Ben-Israel. (2016). Developing Discourse and Tools for Alternative Vontent to Prevent Terror. – In: *National* Security and Counterintelligence in the Era of Cyber Espionage. E. de Silva. (Ed.). Hershey: IGI Global, pp. 102-122.
25. **Simonović,** B. (2004). Kriminalistika. Pravni fakultet, Kragujevac.
26. **Stajić,** Lj. (2005). Osnovi bezbednosti. Fakultet civilne odbrane „Draganić", Beograd.
27. **Strategija** nacionalne bezbednosti Republike Srbije. – In: *Službeni* glasnik RS, br. 94/2019.

ДЕЙНОСТ НА СЛУЖИТЕЛЯ ПОД ПРИКРИТИЕ В ПРЕСТЪПНА ОРГАНИЗАЦИЯ

доц. д-р Руси Янев
Висше училище по сигурност и икономика – Пловдив

UNDERCOVER OFFICER ACTIVITY IN A CRIMINAL ORGANIZATION

Assoc. Prof. Rusi Yanev, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Необходимостта от използване на служител под прикритие в престъпна организация се обуславя от усъвършенстването на схемите и механизмите за извършване на тежки престъпления, предимно с международен характер. Описани са и са обяснени основните компоненти от дейността на служителя под прикритие – подготовка, внедряване, логистично осигуряване, изпълнение на задачите и извеждане от престъпната организация. Очертани са предимствата на дейността под прикритие и основните съдържателни елементи на понятията, използвани в специфичната материя на изложението.*

Ключови думи: *служител под прикритие в престъпна организация; неутрализиране на организирана престъпна група; легенда при оперативно внедряване; логистично осигуряване на служителите под прикритие; доверителна сделка; разследване под прикритие; извеждане на служителя под прикритие*

Abstract: *The need to use an undercover officer in a criminal organization is determined by the improvement of the schemes and mechanisms for committing serious crimes, primarily of an international nature. The main components of the undercover officer's activities are described and explained – preparation, deployment, logistical support, task execution, and removal from the criminal organization. The advantages of undercover work and the main content elements of the concepts used in the specific subject matter of the presentation are outlined.*

Key words: *undercover agent in a criminal organization; neutralizing an organized crime group; legend in operational deployment; logistical support for undercover officers; trust transaction; undercover investigation; taking out the undercover officer*

Необходимост от дейност на служителя под прикритие в престъпна организация

Успешното противодействие на организирани престъпни групи, организации и мафиотизирани структури изисква усъвършенстване на организацията и използване на съвременни методи на оперативно-издирвателна дейност (ОИД). Традиционните методи и специални разузнавателни средства (СРС) невинаги са достатъчно ефективни при разработване на организирани престъпни групи за своевременно разкриване и документиране на сложна и замаскирана престъпна дейност. Резултатите от проведени мероприятия, като вземане на обяснения, изследване на предмети и документи и извършване на насрещни проверки по документи, оперативно наблюдение, идентифициране на лица и обекти, извършване на справки по информационните фондове, за тях все по-често са недостатъчни за установяване и разкриване на организирана престъпна дейност. Съчетаното използване на доброволното сътрудничество с външно наблюдение, подслушване и придобиване на оперативно значима информация от комуникационни средства рядко води до успешна оперативна проверка.

Симбиозата между конвенционална, икономическа и организирана престъпност води до специализация на отделни структури в осъществяване на сложни престъпни схеми с транснационален характер. Придобили икономическа, финансова и нерядко политическа мощ, структурите разширяват престъпната си дейност, като използват защитни механизми за предпазване от правозащитните органи. Контраразузнавателната и оперативно-издирвателна дейност за противодействието им изисква съчетано използване на традиционни със съвременни методи и средства.

Горните обстоятелства наложиха усъвършенстване на ОИД с мероприятия и методи, като контролирана доставка, доверителна сделка и служител под прикритие [3: 107]. При доказана необходимост, когато разкриването на организирани престъпни групи е невъзможно чрез използване на лична издирвателна дейност и екипна работа на специализираните правозащитни структури, СРС и пълния комплекс методи и форми на ОИД и при наличие на обективни възможности, се използва служител под прикритие. За изпълнение на поставени задачи той прониква в обкръжението или в средата на лица, представляващи оперативен интерес, като използва прикритието си за осъществяване на наблюдения върху тях, за получаване на данни за замисляни, подготвяни, извършвани или довършени тежки умишлени престъпления и сложна многоепизодна престъпна дейност.

Необходимост от работа под прикритие в престъпна структура е налице в следните случаи:

а) структурите за сигурност и обществен ред не притежават необходимата информация в обем, достатъчен за разобличаване и последващо неутрализиране на престъпната организация;

б) ръководителите на престъпната организация търсят контрагент за реализиране на неправомерна сделка или дългосрочно сътрудничество в престъпния бизнес;

в) създаване на благоприятна обстановка членове на организацията да се разобличат в извършване на престъпление или в осъществяване на престъпна дейност, чието документиране е било затруднено;

г) за контрол на процеси, чието развитие би довело до вреди и щети в особено големи размери – недопускане на извършването на терористични актове, реализация на големи количества наркотични вещества, пускане в обращение на подправени парични знаци, тежки измами на фондовите борси и др.;

д) обективно, всестранно и пълно разкриване и доказване на извършени и извършващи се тежки престъпления с международен елемент;

е) свидетелстване пред органите на досъдебното производство, съда и при необходимост пред законодателния орган или негови комисии за престъпната дейност на организаторите на престъпното сдружение и негови членове [3: 105 – 108].

Необходимост от дейност на служител под прикритие ще бъде налице и при разработване на транснационална престъпна организация, която използва сложни начини, схеми и механизми за извършване на престъпления с международен елемент, или когато:

а) специализираната правозащитна структура не е получила необходимата информация за реализирани трансакции и търговски сделки със средства от престъпления в обем, достатъчен за разобличаване на всички членове на престъпната организация, след като са използвани възможните за конкретната ситуация оперативно-издирвателни методи и СРС;

б) ръководителите на престъпното сдружение търсят висококвалифицирани лица в областта на счетоводството, финансите и търговските операции за изпиране на пари, контрагенти за реализиране на неправомерни сделки или дългосрочно сътрудничество в легализирането на имуществени стойности;

в) е необходимо създаване на благоприятна обстановка членове на престъпна група да започнат изпиране на пари, след като са осъществявали престъпна дейност, чието документиране е било затруднено.

Понятия, свързани с дейността на служителя под прикритие

За целите на настоящия труд приемаме съдържателните елементи на следните основни понятия, които се използват от компетентни структури, специализирани в използване на служител под прикритие:

- *„служител под прикритие в престъпна организация“* – държавен служител от компетентна правозащитна структура (напр. отдел „Специални операции“ при Главна дирекция „Борба с организираната престъпност“ – МВР), който на принципите на доброволност и специализация се използва при доказана необходимост и при наличие на обективни възможности да проникне в организирани престъпни групи и да осъществява наблюдения върху тях за получаване на данни за замисляни, подготвяни, извършвани или довършени тежки умишлени престъпления и за организацията на дейността им;

- *„организирана престъпна група“ (ОПГ)* – структурирано трайно сдружение на три или повече лица с цел да вършат съгласувано в страната или в чужбина престъпления, за които е предвидено наказание лишаване от свобода повече от три години и чрез които се цели да се набави имотна облага;

- *„разработване на организирана престъпна група“* – осъществяване на комплекс от целенасочени, ефективни и ефикасни оперативно-издирвателни действия, мероприятия и методи под формата на оперативно дело за разкриване и неутрализиране на групата;

- *„разкриване на организирана престъпна група“* – провеждане на оперативно-издирвателни мероприятия за установяване на произхода, структурата, състоянието, участниците, престъпната и легалната дейност на групата;

- *„неутрализиране на организирана престъпна група“* – оперативно-издирвателна дейност за трайно прекратяване на извършването на престъпления от членовете, организаторите и ръководителите на групата чрез прекъсване на връзките между тях;

- *„оперативно внедряване на служител под прикритие“* – използване на съществуващите или на специално създадени благоприятни условия за контакти на служителя с лица от организирани престъпни групи, установяване на доверителни отношения с тях и получаване на сведения в процеса на общуване, необходими за разработване на групите и неутрализиране на престъпната им дейност;

- *„легенда при оперативно внедряване“* – дезинформация на ръководители и членове на разработвани организирани престъпни групи относно истинската самоличност на служителя под прикритие и неговата работа или реалното съществуване на юридическото лице, което той управлява или представлява;

- *„логистично осигуряване на служителите под прикритие“* – система от мерки за материално, техническо и финансово осигуряване на дейността на служителите под прикритие и ефективно ръководство и контрол по разработване на организираната престъпна група с минимален риск за успешното изпълнение на поставените задачи;

- *„лична издирвателна дейност на служителя под прикритие“* – непосредствено прилагане на специфични оперативно-издирвателни методи от страна на служителя под прикритие и осъществяване на целесъобразни мероприятия за разкриване на престъпната дейност на групата;

- *„доверителна сделка“* – привидна ирелевантна сделка с вещ, често забранена за притежание и/или разпореждане, при която служителят под прикритие е едната

страна (обикновено купувач) и я сключва с цел спечелване на доверието на другата страна, действаща от името или за сметка на организирана престъпна група;

- *„разследване под прикритие“ („разследване чрез служител под прикритие“)* – решаване на конкретни задачи и изпълнение на задължения от служител под прикритие в неотложни случаи по искане на прокурор или по разпореждане на наблюдаващ конкретно досъдебно производство прокурор, когато това е единствената възможност за осъществяване на пълно разследване;

- *„операция под прикритие“* – съгласувани оперативно-издирвателни действия и мероприятия на звена, осигуряващи логистична подкрепа на служителя под прикритие за провеждане на реализацията на оперативната разработка за разкриване и документиране на престъпната дейност на организираната група, в която той е внедрен;

- *„извеждане на служителя под прикритие от ОПГ“* – оперативна комбинация за напускане на групата от служителя след изпълнение на задълженията и решаване на задачите или при непосредствена опасност от разконспириране и/или за живота, здравето или имуществото на него или на неговите близки [2: 44].

Компоненти от дейността на служителя под прикритие

Предимства на дейността под прикритие

Предимствата на дейността под прикритие в ОПГ са свързани със следните качества на служителя:

- той е свидетел на замисъла, подготовката, а в определени случаи е и реализатор на отделни епизоди от организираната престъпна дейност и като такъв може да депозира достоверни и надеждни показания пред органите на разследването и на съдебната власт;

- внедреният служител е обучен да изпълнява професионално задачите в престъпната структура, специализиран е в разкриване на отделни престъпления и може да взима относително самостоятелни решения в екстремни ситуации;

- чрез разследващия под прикритие може детайлно и качествено да се планират и осъществят конкретни тактически оперативно-издирвателни действия по реализацията на оперативната разработка за неутрализиране на дейността на престъпна организация.

Подготовка на служителя за работа под прикритие

Неизменен структурен елемент на институционалната страна на организацията на ОИД за разкриване на организирани престъпни групи чрез служител под прикритие е оптималната му професионална подготовка като комплекс от знания, умения и навици. Осигуряването на необходимата квалификация на служителя за противодействие на подготвяни, извършвани и осъществявани тежки умишлени престъпления от престъпни групи и организации е важна задача в обучителната дейност на специализираното звено за работа под прикритие. Своевременността на получаването и детайлизацията на проверката на оперативна информация за дейностите на организираните престъпни групи в голяма степен зависи от квалификацията на служителя под прикритие. Това изисква перманентни усилия за повишаването ѝ, за да се вземат управленски решения, при които се отчитат действията на различните фактори, обуславящи оперативната обстановка.

Обучението на служителя под прикритие е продължителен процес на формиране, поддържане и развитие на умения и навици, психическа устойчивост и делови качества за оптимално осъществяване на личната издирвателна дейност. Определящо значение имат професионализмът, равнището на съзнателност и моралът. Те са предпоставки за повишаване на ефективността на използваните форми и методи на специалната подготовка.

Професионализмът на служителя под прикритие отразява умението му да определя източниците на значима информация за дейността на организираната престъпна група и в зависимост от вида им да я придобива чрез разузнавателно майсторство – установяване на доверителни отношения с лицата, представляващи оперативен интерес, знаещи за престъпната дейност, или ако се касае за други източници – да е във възможност да ги издири и експлоатира. И своевременно да предава информацията на ръководещия го служител във вида, в който я е получил.

Както професионализмът като посочено умение, така и равнището на съзнателност и моралът на служителя са свързани с възпитателното въздействие върху него. Възпитанието на служителя под прикритие е специално организирано въздействие от неговия ръководител или водещия го служител върху съзнанието, волята и чувствата му, съобразено с неговото отношение към работата под прикритие с цел формиране или развиване на качества, които да допринесат за изпълнение на задачите. От обективна страна всяко въздействие върху служителя под прикритие е трудно да се приеме безрезервно, защото се очаква да се анализира и съпоставя с други възприятия, с личния и професионалния му опит като държавен служител, да се оцени и да е предмет на субективни изводи и обобщения. За да се преодолее тази трудност, се използва връзката между възпитанието изобщо и специалното възпитание на служителя под прикритие. Чрез общото възпитание, преди да придобие статута на служител под прикритие, той получава специфични знания за вида и методите на осъществяване на оперативно-издирвателните мероприятия, за използването на доброволни сътрудници и СРС, за особеностите на задачите, които се решават чрез оперативно-издирвателна дейност.

Специалното възпитание е непрекъснат процес, който обхваща съществени и несъществени връзки между различни събития при работата под прикритие и има за цел усъвършенстване на личните и професионалните качества и свойства на служителя, от една страна, а от друга – ограничаване на негативното влияние на средата на действие на организираната престъпна група, в която е внедрен. За осъществяване на резултатно възпитателно въздействие, своевременно трябва да се установяват степента на обусловеност на връзките и евентуалните закономерности при проявлението им.

Възпитателното въздействие и подготовката на служителя под прикритие обуславят един и същ процес на способност за лична издирвателна дейност в ОПГ. Те не трябва да се изолират, но не трябва и да се отъждествяват, защото ще се наруши единството на формиране на специфичната професионална нагласа на служителя. Обучението не решава всички задачи на възпитанието. То има конкретна и познавателна насоченост. Целта му е да се усвоят определени специални знания, навици и умения. Резултатите от него относително лесно се проверяват, докато възпитанието е по-продължителен процес [1: 169].

За да се изпълнят задачите по разкриване на престъпната и привидно легална дейност на разработваната група, професионалните качества на служителя под прикритие, като конспиративност, съобразителност, инициативност, дисциплинираност, трябва да се развиват под влиянието на предварително оценените му лични качества – убеденост в необходимостта за работа под прикритие, степен на съзнателност за неотклонно изпълнение на задачите, имайки предвид особеностите на характера.

Внедряване на служители под прикритие в ОПГ – методи и легендиране

Оперативното внедряване на служител под прикритие в организирани престъпни групи се реализира при спазване на изисквания както от правно, така и от педагогическо и психологическо естество. Изпълнението им в процеса на решаване на поставените задачи е до голяма степен гаранция и за проява на оперативно майсторство.

Внедряването на служителя се осъществява по два основни метода – чрез доброволен сътрудник и самостоятелно. За да не бъде приет с подозрение от организаторите и членовете на престъпната група, наличен сътрудник, ползващ се с доверие в организацията, представя служителя под прикритие с необходимите препоръки. Според оперативната необходимост след внедряването на полицейския орган сътрудникът може да бъде изведен от престъпната организация. Самостоятелното внедряване предполага по-продължителен период на работа под прикритие извън престъпната организация с цел създаване на авторитет сред престъпните среди. Служителят под прикритие може да бъде потърсен от членове на престъпната организация за съвместна дейност или може сам да търси контакти с ръководителите на организацията с конкретни предложения. И в двата случая легендата за оперативното внедряване трябва да бъде изградена и осигурена по всички правила на оперативното майсторство. В някои от особено опасните престъпни сдружения, за да приемат нов член, той трябва да извърши престъпление под наблюдението на доверено лице на ръководството или на самия ръководител. За внедряване в такива сдружения се използва перфектно планирана и изпълнена оперативна комбинация.

Дейността на служителя под прикритие като член на престъпно сдружение е рискована. Всяка грешка в поведението и действия извън легендата може да застраши живота му. Престъпната среда въздейства натоварващо и сложно на психиката на служителя. При дълбоко конспириране съществува реална опасност от промяна в мисленето, възгледите и действията на служителя като лице от престъпния свят.

Логистично осигуряване на работата под прикритие в ОПГ

За да бъде успешна работата под прикритие, е необходимо непрекъснато логистично осигуряване на служителя. Изградената легенда се поддържа чрез прилагане на мерки и извършване на действия от различни служители за материално, техническо и финансово осигуряване на изпълнението на задачите по разработване и неутрализиране на престъпната група и организация.

Мерките и действията обхващат:

- изготвяне на документи: за самоличност – лична карта, паспорт, свидетелство за управление на МПС с променени имена на служителя под прикритие; регистрационни документи на различни търговци – съдебна, данъчна и осигурителна, митническа; регистрационни документи на МПС и др. необходими;
- формиране на екипи от служители за поддържане на изградена легенда;
- осигуряване на служителя под прикритие с техника за заснемане, записване, маркиране на предмети и др.;
- осигуряване на парични средства за поддържане на легендата при внедряването и изпълнението на задачите по разработване на ОПГ.

Извеждане на служителя под прикритие от ОПГ

Предпоставки за извеждане

Оптималният резултат от работата под прикритие е разкриване и неутрализиране на ОПГ. От една страна, в условията на личната издирвателна дейност или разследването под прикритие поставените задачи на служителя могат да бъдат изпълнени успешно. Така необходимостта от неговото използване като служител под прикритие отпада. Но от друга страна, като се има предвид характеристиката на средата в ОПГ, свързана с напрежение и рискове, може да възникне опасност от разконспириране или непосредствена заплаха за здравето и живота на служителя, негови близки или тяхното имущество.

При наличието на горните предпоставки възниква необходимостта от извеждане на служителя от ОПГ, където е внедрен. Извеждането е свързано с осъществяване на оперативна комбинация за недопускане или разколебаване на членовете, организаторите или ръководителите на ОПГ да възникне или да се развие съмнение за причастност на служителя към правозащитна структура.

Начини на извеждане

Начините на извеждане на служител под прикритие от ОПГ зависят както от действия на самия служител и логистичен екип, така и от случайни събития. Познати са следните начини на извеждане:

а) Създаване и поддържане на заблуждение у членовете на ОПГ, че разкриването им е вследствие на тяхната непредпазливост при подготовката, извършването и прикриването на престъпната дейност. Използват се обстоятелства, които са възникнали по естествен път и са спомогнали за провеждане на оперативна комбинация за извеждане. Целта е да се създаде убеждение в ОПГ, което изключва възможността за съмнение относно служителя под прикритие, че разкриването е в резултат на неговата работа.

б) Създаване и поддържане на заблуждение у членовете на ОПГ, че разкриването им е в резултат на случайни събития, довели до провал на престъпните действия. Създаването на убеждение за ролята на случайните събития изключва опасността от подозрение на служителя под прикритие.

в) Използване на легенда – заминаване на служителя по направление извън местата на реализация. Целта е изключване на съмнение, че той е съобщавал на полицията за престъпната дейност. За прилагането на начина е необходимо да се спазват следните изисквания:

- заминаването да се реализира известно време преди реализацията, а не непосредствено преди нея;
- в ОПГ предварително да са информирани за необходимостта и причините на заминаването;
- поводът за заминаването да бъде ясен, точен и убедителен;
- по възможност реализацията да започва по повод, който привидно не е могъл да бъде известен на служителя под прикритие, за да отпадне от него всякакво съмнение.

г) Създаване на убеждение у разработваните лица, че разкриването на организираната им престъпна дейност е вследствие на признанията на някои от тях.

д) Задържане на членове на ОПГ при извършване на престъпление или непосредствено след извършването му с веществени доказателства. Служителят под прикритие напуска групата, като декларира пред останалите членове, че ще се укрие, защото се опасява, че ще бъде предаден от задържаните.

е) Показно задържане на служителя под прикритие пред членове на ОПГ, отвеждане в неизвестна за разработваните лица посока и дезинформиране на групата, че на служителя е повдигнато обвинение.

Заключение

Ограничаването на предизвикателствата, рисковете и заплахите за националната сигурност от организирана престъпна дейност често е свързано с работа под прикритие на специализирани държавни служители на компетентни правозащитни структури. Това е работа, изпълнена с висок риск за здравето, живота и имуществото на служителя и неговите близки. Осигуряването на законосъобразно използване на служителя под прикритие е до голяма степен гаранция за успешно разследване на тежки престъпления, предимно с международен елемент, извършвани от организирани престъпни групи, организации и мафиотизирани структури.

Литература

1. **Каймеджиев,** Христо. Теория на оперативно-издирвателната дейност. Част втора. София: ВИПОНД-МВР, 2000.
2. **Янев,** Руси и кол. Противодействие на организираната престъпност. София: АМВР, 2011.
3. **Янев,** Руси. Международно сътрудничество за противодействие на тежката и организираната престъпност. – В: *Научни* трудове на ВУСИ, том IX, 2023 г. Пловдив: ВУСИ, 2024.

ПЕРСПЕКТИВИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД БЪЛГАРСКАТА ДИПЛОМАТИЧЕСКА СЛУЖБА В УСЛОВИЯТА НА СЪВРЕМЕННАТА ГЕОПОЛИТИЧЕСКА ДИНАМИКА

доц. д-р Пламен Теодосиев
Университет по библиотекознание и информационни технологии – София

PROSPECTS AND CHALLENGES FACING THE BULGARIAN DIPLOMATIC SERVICE IN THE CONTEXT OF CONTEMPORARY GEOPOLITICAL DYNAMICS

Assoc. Prof. Plamen Teodosiev, PhD
University of Library Science and Information Technology – Sofia

Резюме: *Докладът анализира ключовите предизвикателства и стратегически перспективи пред българската дипломатическа служба в условията на съвременната геополитическа динамика. Разглеждат се глобалните процеси на конфронтация между Великите сили, регионалната нестабилност и хибридните заплахи, като се подчертава нуждата от модернизация, професионализация и по-активно участие в международните инициативи. Направени са конкретни препоръки за подобряване на капацитета на дипломатическата система, развитие на публичната дипломация и дигитализация на институционалната рамка.*

Ключови думи**:** *българска дипломация; геополитика; международни отношения; хибридни заплахи; ЕС; НАТО; публична дипломация*

Abstract: *The report analyses the key challenges and strategic perspectives for the Bulgarian diplomatic service in the current geopolitical dynamics. It has examined the global processes of the great Powers, regional instability and hybrid threats, highlighting the need for modernisation, professionalisation and more active participation in international initiatives. Specific recommendations are made to improve the capacity of the diplomatic system, develop public diplomacy and digitalize the institutional framework.*

Key words: *Bulgarian diplomacy; geopolitics; international relations; hybrid threats; EU; NATO; public diplomacy*

Увод

Българската дипломатическа служба като част от външнополитическия апарат на Република България играе ключова роля в защитата на националните интереси, поддържането на международните отношения и реализирането на външната политика на страната. В условията на съвременната геополитическа динамика, характеризираща се с нестабилност, нарастващи глобални конфликти, хибридни заплахи и конкуренция между Великите сили, дипломацията е призвана да бъде по-адаптивна, проактивна и стратегическа.

Геополитически контекст и глобални тенденции

Съвременният геополитически пейзаж се характеризира с ускорени трансформации, полицентризъм и ескалираща конкуренция между глобални и регионални сили. Появяват се нови конфликти, съществуващите се задълбочават, а институционалните механизми за управление на международната сигурност са под натиск. През последните години наблюдаваме увеличаване на влиянието на държави, като Китай,

Индия, ОАЕ и Саудитска арабия. Тези сили се стремят да променят традиционната система на глобалната сигурност, което води до предизвикателства за държавите от по-малки мащаби. Светът се движи към мултиполярна структура, в която политико-икономическите съюзи имат влияние върху глобалните процеси. България трябва да адаптира своята външна политика към новата реалност, като прецизира своите позиции и интереси в контекста на многостранната дипломация.

Възраждане на глобалната конфронтация

След десетилетия на относителен международен консенсус светът се връща към логиката на блоковото противопоставяне. Отношенията между САЩ и Китай се влошават поради търговски спорове, технологично съперничество и сблъсъци в региона на Тайван. В същото време войната в Украйна представлява фундаментален разлом между Русия и Запада. ЕС и НАТО засилват външната си политика и сигурност, докато Русия и Китай изграждат паралелни структури за влияние. В регионален план противоречивата външна политика, която води Турция, също създава известни безпокойства. Това изисква българската дипломация да бъде едновременно балансирана и лоялна към съюзническите ангажименти.

Регионални конфликти и нестабилност

Черноморският регион, в който България има директна географска ангажираност, е зона на засилено военно присъствие, енергийна конкуренция и стратегически интереси на трети страни. Западните Балкани остават чувствителни към етнически, политически и религиозни напрежения. България има интерес от стабилност, европейска интеграция и предотвратяване на враждебни влияния в региона. В същото време Близкият изток и Северна Африка остават източник на миграционен натиск и трансгранични рискове, които влияят върху външната политика на страната.

Хибридни заплахи и глобални предизвикателства

Хибридната война се превърна в предпочитан инструмент за държави, които не могат или не желаят да водят открита военна конфронтация. Дезинформация, кибератаки, икономическо проникване, енергийна зависимост, културно и религиозно влияние – всички тези форми на нестандартна намеса изискват многоизмерен дипломатически отговор. Освен това глобалните предизвикателства, като климатични промени, пандемии, технологични трансформации и ресурсна конкуренция, също изискват включване на България в международни формати и коалиции с дългосрочен хоризонт.

Основни предизвикателства пред българската дипломатическа служба

Българската дипломатическа служба се сблъсква с редица системни, функционални и институционални предизвикателства, които ограничават способността ѝ да бъде стратегически ефективна и проактивна в международната среда.

Недостатъчен капацитет – човешки и финансов

Дипломатическата мрежа на България остава една от най-малките в ЕС. Често дипломатически мисии се състоят от минимален персонал с множество функции. Недостатъчното финансиране води до затруднения при представителството, логистичната поддръжка и участието в международни събития. Освен това липсва устойчив модел на подбор и развитие на кадри. Подготовката и усъвършенстването на кадри се

осъществява единствено чрез Дипломатическия институт към МВнР, чийто капацитет е недостатъчен.

Политизация и непоследователност

Назначенията по политически линии и честа смяна на външнополитическите приоритети водят до несигурност и липса на дългосрочна визия. Това подкопава доверието на международните партньори и намалява експертизата вътре в системата. Дипломацията се нуждае от професионализация, деполитизация и стабилност.

Слабо стратегическо планиране и координация

Липсва цялостна външнополитическа стратегия, която да обвързва приоритетите на различните институции и да гарантира координация между външната политика, отбраната, икономиката и културата. Това води до разнопосочни инициативи, които не носят синергичен ефект.

Неизползван потенциал на публичната и дигиталната дипломация

Съвременната дипломация изисква активно присъствие в цифровите канали, мобилизация на диаспората, участие в международни дебати и сътрудничество с гражданското общество. България все още не е развила пълноценна система за публична дипломация, насочена към изграждане на положителен образ и влияние.

Дезинформация, киберзаплахи, икономически натиск и намеса във вътрешни политически процеси се превръщат в основни инструменти за влияние от страна на враждебни сили. Дипломацията трябва да работи в координация с други институции – разузнаване, отбрана, вътрешна сигурност – за изграждане на устойчиви механизми за отговор.

Перспективи на развитие

Въпреки настоящите трудности българската дипломатическа служба има потенциал да се утвърди като ефективен и авторитетен участник в международните отношения, при условие че бъдат реализирани реформи и стратегическо преосмисляне на ролята ѝ.

Превръщане на България в активен участник в ЕС и НАТО

България може да бъде фактор в регионалната сигурност, енергийната устойчивост, киберсигурността и миграционната политика. Участието в съвместни европейски инициативи, механизми за стратегическа автономия и коалиции по интереси ще увеличи международната ѝ тежест. В НАТО България трябва да играе активна роля в южното и източното флангово планиране.

Разширяване на регионалната дипломатическа инициатива

България може да бъде катализатор за координирани действия в Югоизточна Европа чрез формати, като Процеса за сътрудничество в ЮИЕ, Инициативата „Три морета“ и др. Дипломацията може да поддържа активни връзки с балканските държави, Гърция, Турция и черноморските партньори.

Дигитализация и институционална модернизация

Необходима е тотална реформа на Външното министерство – преминаване към електронни платформи, интегрирани комуникационни системи, автоматизация

на рутинните дейности и използване на изкуствен интелект за анализ на международните процеси.

Професионализация и инвестиция в човешкия капитал

Създаване на устойчива дипломатическа академия с международно участие, привличане на млади експерти, програми за специализация и обучение в сферата на дигиталната дипломация, киберполитика, икономическа дипломация и международно право.

Възстановяване и разширяване на публичната дипломация

Изграждане на мрежа от културни центрове, стратегическо присъствие в социалните медии, включване на научната и академичната общност в публичната комуникация на България. Това ще допринесе за изграждането на международен авторитет и доверие.

Развитие на икономическата дипломация

Посолствата и консулствата трябва да играят активна роля в привличането на инвестиции, насърчаването на търговията и представянето на България като бизнес дестинация. Тясно сътрудничество с Министерството на икономиката и бизнеса е от решаващо значение.

Използване на „меката сила“

Българската култура, история, образование и туризъм са мощни инструменти за изграждане на международен авторитет. Разширяването на програмите за културен обмен, стипендии и съвместни научни проекти ще подобри имиджа на страната в чужбина.

Препоръки

- Разработване на национална външнополитическа стратегия и визия за дипломатическа дейност с хоризонт поне 10 години. В процеса да бъдат привлечени основно експерти, бивши дипломати с широк международен и регионален опит, преподаватели.
- Увеличаване на бюджета за дипломатическата служба и подобряване на условията на труд.
- Създаване на Център за стратегически анализ към МВнР, в който да участват външни експерти.
- Повишаване на експертността чрез постоянно обучение и включване на външни специалисти.
- Засилване на публичната дипломация чрез модерни комуникационни канали и медийно присъствие.
- Изследване на възможностите за приложение на изкуствен интелект и предлагане на модели за приложението му в дипломатическата служба.

Заключение

Българската дипломатическа служба е стратегически инструмент за гарантиране на националната сигурност, икономическо развитие и културно влияние. Предизвикателствата на съвременната международна среда изискват нейното спешно об-

новяване, професионализация и стратегическа ориентация. Чрез ясни приоритети, модерни инструменти и ефективно ръководство България може да затвърди позицията си на стабилен и предвидим партньор на международната сцена.

Използвани източници

1. **Министерство** на външните работи на Република България. (2023). Годишен доклад за външната политика.
2. **European** External Action Service (EEAS). (2023). EU Strategic Compass for Security and Defence.
3. **NATO.** (2023). Strategic Concept 2022.
4. **Council** of the European Union. (2023). EU enlargement policy and the Western Balkans.
5. **Carnegie** Europe. (2023). Europe's Eastern Neighborhood in Flux.
6. **Center** for the Study of Democracy. (2023). Bulgaria's Vulnerability to Hybrid Threats.
7. **UNESCO.** (2022). The Role of Cultural Diplomacy in International Relations.
8. **Harvard** Kennedy School. (2021). Digital Diplomacy: Technology and International Engagement.
9. **Brookings** Institution. (2023). Revitalizing the Foreign Service in the 21st Century.

ДЕОНТОЛОГИЯ НА СЛУЖБИТЕ ЗА СИГУРНОСТ И ОБЩЕСТВЕН РЕД

доц. д-р Петър Тодоров
Висше училище по сигурност и икономика – Пловдив

DEONTOLOGY OF SECURITY AND PUBLIC ORDER SERVICES

Assoc. Prof. Petar Todorov, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Деонтологията на службите за сигурност и обществен ред представлява наука за правилното упражняване на служебната дейност и поведението на държавните служители – административния апарат, професионалистите, изпълняващите най-важните функции за обществото, свързани с възложената им мисия – да осигурят сигурността и опазването на обществения ред в страната, като реализират по най-целесъобразен начин дадените им правомощия на държавни органи. Формулирането на този проблем е от значение за прилагане на ценностите на правовата държава и в тази връзка може да се каже, че в една правова социално ориентирана държава държавната служба играе значителна роля. Следователно държавните служители в службите за сигурност и обществен ред трябва да разберат своята цел, да почувстват своята съпричастност към решаването на държавни проблеми, да работят упорито, изпълнявайки дълга си към народа и държавата.*

Ключови думи: *деонтология; етика; държавна служба; сигурност; обществен ред*

Abstract: *The deontology of the security and public order services is a science of the proper exercise of official activity and the behavior of civil servants – administrative apparatus, professionals performing the most important functions for society, related to their assigned mission – to ensure security and preservation of public order in the country, by implementing in the most expedient manner the powers given to them by state bodies. The formulation of this problem is important for implementing the values of the rule of law, and in this regard it can be said that in a legal socially oriented state the civil service plays a significant role. Therefore, civil servants in the security and public order services must understand their purpose, feel their involvement in solving state problems, work hard, fulfilling their duty to the people and the state.*

Key words: *deontology; ethics; civil service; security; public order*

„Деонтология или науката за морала“

„Deontology or The Science of Morality“ е произведение на Джереми Бентъм – основателя на утилитарната морална философия. Посветено е на основния въпрос на утилитаризма[1]: какво трябва да се направи за най-голямо щастие на най-голям брой хора. За да обозначи утилитарната система на етиката, Бентъм въвежда ново понятие – „деонтология“ (от гръцки „δέον“ – „дължимо, правилно, трябва“), като учение за правилното, дължимото поведение. Основата на деонтологията е принципът на полза, според който дадена постъпка заслужава или не заслужава одобрение в зависимост от нарастването или намаляването на „сумата на социалното щастие“. Първата част, посветена на теорията за добродетелта, разглежда връзката между интереса и дълга, концепцията за деонтологията, връзката на удоволствието и болката с доброто и злото,

[1] *утилитарѝзъм,* -змът, -зма, мн. няма, м. (лат.). 1. Филос. Етическо учение, което смята за основна цел на личната и обществена нравственост ползата, тесния практицизъм. 2. Прен. Книж. Стремеж да се извлича от всичко само непосредствена материална изгода, Речник на съвременния български книжовен език (онлайн).

ролята на санкциите, причините за неморалността, дефиницията на добродетелта, благоразумието, положителните и отрицателните аспекти на милосърдието, анализ на добродетелта и порока, страстите и интелектуалните способности и историята на принципа на щастие. Втората част разглежда практиката на добродетелта, особено благоразумието и милосърдието. Задачата на деонтологията е да даде на социалните мотиви цялата сила на личните мотиви, да убеди, че личните интереси и задължения към обществото съвпадат, а желанието за собствено щастие, егоизмът на хората като силни мотиви са необходими за осигуряване на съществуването на човечеството и в комбинация с разума могат да служат на социалното щастие. Чувството на симпатия е много важно, разширявайки нашия „Аз“ до колективен „Аз“, което ни позволява да „живеем двойно“ – в себе си и в другите и в комбинация с интелектуалните способности на лидерите, морално подобряване и намаляване на различни санкции. Развивайки утилитарни идеи, Бентъм допринася за обсъждането на класическия принцип на полезност, връзката между интерес и дълг, ролята на законодателя и доктрината за психологическия егоизъм в моралната философия [2].

Етика и деонтология

Деонтологичната етика се фокусира върху моралните принципи, а не върху моралността на резултатите от взетото решение. Не бива да се слага знак на равенство между етиката и деонтологията на определена професия. Ако в етиката се третират законите, наредбите и инструкциите, които определят правата и задълженията на професионалистите като граждани на определено общество (държавата), то в деонтологията се включват онези морални ценности и норми, които са не само специфични за професията, но и стоят над приетите закони в обществото.

Дългът е една от основните категории на етиката, тъй като сферата на морала е сферата на това, което трябва да се направи (да бъдем честни, да бъдем справедливи и т.н.). Дългът е социална необходимост, изразена в морални изисквания към индивида. С други думи това е превръщането на общо морално изискване в лична задача за конкретен човек, формулирана във връзка с неговата позиция и конкретна ситуация. Дългът отдавна е получил специално признание в дейността на служителите от службите за сигурност и обществен ред.

Професионалното задължение на държавните служители от посочените служби е съвкупност от правни и морални изисквания, наложени им при упражняване на техните правомощия. По този начин професионалният и моралният им дълг изключват забавяне или отказ да се реализират дейности по защита на националната сигурност и опазване на реда в страната. Като неразделна част от обществения дълг професионалният дълг на служителите е в основата на моралните отношения в професионалната им дейност.

Професионалните задължения на тези служители имат обективна и субективна страна. Моралната стойност на обективното съдържание на дълга (обективната страна на дълга) е, че то е подчинено на решаването на най-висшата и най-справедлива задача: защита на правата на личността, осигуряване на законност и ред в страната. Обективната страна на задължението представлява ясно формулирани задачи, поставени от държавата и закрепени в законови норми, регламентиращи дейността на службите за сигурност и обществен ред.

Моралната стойност на дълга в неговия субективен израз се проявява в случаите, когато социалните задължения, определени от държавата на тези служители, се възприемат като справедливи и верни, признават се от тях като лични дълбоки нужди и убеждения и се превръщат в доброволна и целенасочена дейност. Субективната

страна на дълга е вътрешна убеденост в справедливостта и правотата на каузата, на която човек посвещава живота си.

Професионалното задължение на държавния служител в службите за сигурност и обществен ред е фокусът на връзката между целия набор морални норми и принципи, от които се ръководи, и неговата професионална практическа дейност. Дългът разкрива активната природа на морала, която се състои в превръщането на морално осъзнатото в постижимо. В дълга теорията се трансформира в практика, моралните принципи и норми – в реални действия и постъпки. Професионалният дълг мобилизира служителя или групата служители да изпълняват дейността си ефективно, навреме, с най-ефективен резултат и ги принуждава да използват всичките си физически и морални сили за постигане на целите си. Професионалните им задължения се определят от взаимодействието на правните норми и моралните норми, тъй като моралните норми регулират вътрешното съзнание на човека за неговото поведение, а правните норми регулират външната форма на поведение. Изискванията на професионалното задължение са законово закрепени в закони, наредби, правилници и инструкции. Например изискванията на правно формализиран дълг, изразени в полаганата клетва при постъпване на държавна служба, съдържат както морална оценка, така и правна норма. В сферата на професионалния дълг няма законови изисквания, лишени от морална сила, както няма морални норми, които нямат правна сила. Следователно в професионалния дълг юридическите и моралните аспекти се сливат в едно.

Професионалното задължение на служителите не може да се отъждествява с тяхното правно задължение. Правното им задължение е свързано с тяхната компетентност, която е ясно определена от нормите на специалните закони и включва държавна принуда под формата на различни правни санкции в случай на нейното неспазване. Понятието „професионално задължение“ е по-широко по обхват от правното задължение. Професионалното задължение се различава от задълженията с правно естество по това, че включва както правни задължения, така и определени морални изисквания (задължения), произтичащи от реализираната от тях дейност. Професионалният дълг се осъществява не от принудителната сила на държавния контрол, а въз основа на вътрешното убеждение, повелята на съвестта, справедливостта, признати като вътрешна необходимост. Например професионалното задължение на служителите (морално задължение и задължение от правно естество) е да установят и правилно да оценят фактите, които показват, че има вероятност конкретни лица да са наясно с различни по вид обстоятелства, свързани със случая, по който работят. В същото време е необходимо да се изключи неоснователното призоваване за снемане на сведения, което води, от една страна, до безпокойство у гражданите, а от друга, до загуба на собствено време.

Или друг пример, свързан с професионалното задължение на държавния служител към лицата, даващи вярна информация по случаите, които представляват професионален интерес. За да бъдат убедени, че се прави всичко възможно да бъдат защитени техните интереси, тайна или права, служителят трябва от време на време да ги уведомява/информира за статута на конкретния случай и ако е уместно, да се срещне с тях в среда, различна от кабинета в държавното учреждение. Независимо какви функции изпълнява служителят, има много ситуации, в които не може да бъде контролиран пряко отвън. Нито силата на правното влияние, нито влиянието на колегите, ако не съвпадат с вътрешни лични мотиви, убеждения и съвест, могат да бъдат гаранция, че в хода на дейността си конкретният служител няма да наруши професионалния си дълг. Следователно най-важният елемент на моралния дълг е самодисциплината.

Механизмът на самодисциплината (самоконтрола) обхваща: убеждения на индивида, постепенно развиващи се в процеса на социална дейност; чувства; навици; са-

мооценка на човек за собствените му действия, мотиви и морални качества; самообразование. Необходимо е такова високо ниво на развитие на моралното отношение към дълга, като всяко едно действие се съобразява и не влиза в противоречие със самосъзнанието, а изпълнението на дълга е подкрепено от повелите на съвестта, като дисциплината като основен израз на професионалния дълг се превръща в самодисциплина.

Самодисциплината действа като вътрешна готовност да се следват изискванията на закона, клетвата и заповедите на ръководството, възприемани като вътрешни мотивации, като необходимост. Най-правилното нещо, което обществото може да изисква от един служител в службите за сигурност и обществен ред, е желанието да изпълнява професионалния си дълг не под натиск (независимо от кого идва), а с чиста съвест, доброволно. Следователно самодисциплината е високоморално поведение, което се извършва въз основа на дълг и съвест.

За правилното изпълнение на професионалния дълг са от голямо значение морални фактори, като съвест, чест и репутация. Съвестта е вътрешно съзнание за морален дълг и отговорност към обществото, което изисква самоконтрол от индивида, стриктно спазване на нормите на лично и служебно поведение и самокритична оценка на собствените действия. Тук дългът и отговорността към себе си са неразривно свързани. Съвестта на индивида като цяло и на служителя в частност се проявява в различни форми:

1. морално удовлетворение (изпълнено задължение; помощ на човек в нужда; защита от атаките на престъпник);

2. чувство на срам (при извършване на неморално действие, станало известно на някого; действия, които са известни само на лицето, което ги е извършило).

Понятието „чест“ разкрива отношението на човек към себе си и отношението на обществото към него. То играе същата роля в човешките взаимоотношения и регулирането на поведението на индивида като достойнството. В Преамбюла на Международния пакт за граждански и политически права се посочва, че човешкото достойнство е присъщо качество на всички членове на човешката раса, от което произтичат всички неотменими права и от което се основават свободата, справедливостта и универсалният мир [2].

Моралната стойност на човек в понятието „чест“ се свързва със специфичното положение на човек, вида на неговата дейност и моралните заслуги, които му се признават. За разлика от понятието „лично достойнство“, което се основава на принципа на равенство на всички хора в морално и правно отношение, понятието „чест“, напротив, оценява хората по различен начин. Тази оценка се отразява на репутацията. Съответно честта изисква човек да поддържа репутацията, която има, или тази на екипа, в който работи.

Професионалната чест е движещата сила на всички морални действия, които се проявяват при изпълнение на професионалния дълг. Честта на служителите от службите за сигурност и обществен ред е неделима от честта на екипа, в който работят. Следователно те не трябва да си позволяват да извършват действие, което би опозорило техните колеги.

Понятието „професионална чест“ понякога е тясно свързано с понятието „амбиция“. Всеки държавен служител трябва да има здравословна амбиция, тъй като тя определя желанието да се заеме място в йерархичната служебна пирамида, което да отговаря на способностите и цената на труда. Правилно разбраната амбиция не вреди на общата кауза, а напротив, дава допълнителна сила за нейното осъществяване. Здравословната амбиция на служителя се проявява като мотив за действия, които се извършват с цел постигане на първенство, лидерство, придобиване на влияние и тежест, както и с цел получаване на официално признание и свързаните с него почести и награди.

Здравословната амбиция трябва да се идентифицира с концепцията за професионална кариера. За съжаление, този термин е компрометиран от понятието „кариерист“. Професионалната кариера по своята същност е повишение, което се определя от качеството на извършената работа, заеманата длъжност, трудов стаж и други лични заслуги. Всеки вид служебна дейност има своя специфика: група взаимносвързани (вертикално и хоризонтално) длъжности образуват определена кариера. Специалните закони ясно регламентират процедурата за професионално израстване и заемане на по-високи по вид длъжности.

Обратното на здравословната амбиция е кариеризмът, който действа като отрицателно морално качество, което характеризира личността и поведението на човека. Кариеристът е готов да изпълни поставените пред него изисквания само доколкото това допринася за подобряване на личната му позиция и напредък в кариерата. За него житейският принцип не е служене на общата кауза, а външна демонстрация на неговата привързаност към инструкциите на представителите на официалната власт, за да бъде „забелязан“. Най-негативното е, че кариеристът в желанието си да заеме важна позиция е безразличен към съдбата на хората. Ето защо служителите, които имат голям кръг правомощия, докато се движат нагоре по кариерната стълбица, трябва да помнят, че не трябва да използват „мръсни“ средства за постигане на егоистични цели, т.е. трябва винаги да бъдат с „чисти ръце“.

Деонтологията на държавната служба в службите за сигурност и обществен ред

Френският изследовател на проблемите на деонтологията на държавната служба проф. Кристиян Вигуру твърди, че деонтологията „е един от централните елементи на тази „държавност“, от който следва да се ръководи всяко длъжностно лице на държавна служба. Това е нещо повече от професионалната съвест на служителя, работещ за държавата. „Държавността“ следва от конституцията (...) и от необходимостта до известна степен да жертваме собствените си интереси, служейки на обществото“ [5].

Джереми Бентъм в своя труд „Деонтология, или науката за морала“ [4] основава своите възгледи с приоритетно внимание към проблемите на „държавния морал“, който има пряко отношение към правилното изпълнение на обществените задължения на служителите. Той е първият, който предлага за науката модел на норма на професионално поведение на човек, който по силата на своята социална роля е надарен с правомощия на власт и е призован в рамките на етиката да ги прилага в интерес на обществото и конкретни граждани. Мислителят залага на методически обоснован подход към проблемите, свързани с държавната служба, допринася за създаването на система от норми на деонтологията на държавните служители.

Категориите „задължение“ и „подобаващо поведение“ се отнасят, разбира се, не само за професионалната дейност на държавните служители. Те характеризират целия спектър социални отношения на човек, който е поел отговорността да изпълнява държавна служба както в обществения, така и в личния живот. Въпреки това приложният аспект на деонтологията на държавната служба е съзнателно ограничен до обхвата на обекта и предмета на изследване, както и професионалната дейност и поведение на държавните служители.

Обект на изучаване на деонтологията се явяват институтът на държавната служба, дейността и поведението на държавните служители. Основната цел на държавната служба е да задоволи основните потребности на населението на страната и обществото. По този начин деонтологията отговаря на въпросите: каква трябва да бъде държавната служба; какви средства, техники и методи трябва да използва, за да

отговори на нуждите на хората в една нормативно уредена и социално ориентирана държава, в която човекът е най-висшата ценност; как да създадем достойни условия за живот и личностно развитие на хората; какъв трябва да бъде държавният служител; какви личностни качества трябва да притежава; от какви ценности да се ръководи; какви норми и правила на поведение да се следват.

Предметът на всяка наука, както е известно, разкрива различни аспекти на обекта на изследване, определя неговото систематизирано съдържание. Предметът на деонтологията на службите за сигурност и обществен ред обхваща:

1. проблема за съотношението и хармонизирането на правилното и реалното в осъществяването на служебната дейност на държавните служители;

2. изследване на съдържанието на реалното съзнание на социалната професионална макрогрупа на държавните служители, което включва субектно въплъщение (както във форма, така и по съдържание) на ценности, знания, умения, способности, морал, нагласи, потребности, интереси и др.;

3. разработване и кодифициране на норми, изисквания и стандарти за правилно поведение и дейности на държавните служители при изпълнение на техните функционални задължения;

4. проучване на цялото разнообразие на социални отношения и реално поведение на служителите, естеството и методите на тяхната дейност, както и разработване на препоръки за тяхното подобряване;

5. проучване на социалните очаквания и изисквания, предявявани от гражданите към държавните служители, намиране на начини за постигане на съответствие на тяхната служебна дейност и поведение със социалните очаквания, проучване на възможностите за създаване на социално партньорство;

6. разработване и формиране на система за мотивация и стимули на държавните служители за адекватно изпълнение на служебните задължения;

7. изграждане на ефективна система за социален контрол върху дейността и поведението на държавните служители.

Деонтологията като наука наистина може да повлияе върху повишаването на нивото на морала и ефективността на държавните служители в съвременното държавно управление. Това е разбираемо, тъй като представените социални проблеми в цялото им многообразие създават естествено диалектическо единство. Единствен се явява и обектът на приложение на деонтологичните норми – обществото, социалните общности и групи, съставляващите ги индивиди, и преди всичко лицата, които са овластени по силата на своя социален статут и притежават специални правомощия. Дейностите и поведението на държавните служители в деонтологията се представят като съвкупност от всички социални връзки и отношения чрез личността на държавния служител. В тази връзка е възможно да се идентифицират основните фактори (и съответно аспекти на деонтологичния подход), които влияят върху дейността и поведението на държавните служители, а именно: философски, етически, правни, социологически, политически, културни, естетически, психологически, педагогически и др. Всички те намират пряко въплъщение в процеса на държавното управление и чрез него спомагат за решаването на социални проблеми.

Подчертавайки общата необходимост от деонтология, К. Вигуру счита за необходимо да се утвърдят позитивните принципи на дейността на държавните служители, които трябва да се основават на законов механизъм за контрол и санкции. Предлагат се принципи – общи за всички видове публични услуги: равенство и свобода, приемственост, безпристрастност, неутралност, зачитане на религиозните вярвания, зачитане на морала и добрите нрави, безплатни услуги, знание за крайни резултати и обществена полза, делегиране на правомощия, защита на потребителя [5].

Деонтологията на службите за сигурност и обществен ред, от една страна, е институционализирана чрез създадените и обнародвани етически кодекси, правилници и създадени стандарти в Р България, но от друга страна, институционализирането на всяка наука предполага създаването на теории и концепции, обосновка на категориален апарат, дефиниране на обект и предмет на изследване, изясняване на моделите на социалната реалност и др. За да се решат голямата част от въпросите, свързани с обучението на служителите, е необходимо да се реализират множество научни публикации, свързани с деонтологията, да се разработят учебници и учебни помагала, позволяващи осъществяването на деонтологично обучение на кадри за службите за сигурност и обществен ред.

В заключение е важно да се отбележи, че появяването на обществена потребност от разработването на деонтология на службите за обществен ред и сигурност в страната е обективно обусловено изискване на съвременността.

На първо място, в правовите демократични и социално ориентирани държави служителите от службите за сигурност и обществен ред са задължени да приведат в съответствие своя висок социален статут към образа на достойното изпълнение на служебните задължения, служейки на гражданите на Р България. Именно в това направление е насочена деонтологията на държавната служба в специализираните държавни органи, гарантиращи националната сигурност и опазващи обществения ред.

На второ място, налице е обществена осъзнатост на факта, че благосъстоянието на хората и чувството им за сигурност е в пряка зависимост от деонтологичния потенциал на държавните служители, очаквайки от тях подходящо и правилно професионално поведение, спазване на общоприетите професионални етически и деонтологични стандарти.

На трето място, деонтологията като система от принципи, изисквания, норми, дължимо професионално поведение, като теоретична и практическа, научна и образователна дисциплина може да отговори на социалната потребност за изграждане на система от научни знания за дължимото към обществото поведение от страна на служителите от службите за сигурност и обществен ред. На тази наука е генетично присъща връзката между етиката и правото с приоритетен акцент върху проблемите на „държавния морал“.

На четвърто място, деонтологията може да способства за изграждането на обществено приемлив образ на тази голяма професионалноориентирана група държавни служители, като им предостави така необходимата система от социални (етически, правни, организационни, управленски, културни и др.) норми, стандарти и изисквания, насочени към качественото функциониране на службите за сигурност и обществен ред в Р България.

Използвани източници

1. **Международен** пакт за граждански и политически права. Ратифициран с Указ № 1199 на Президиума на Народното събрание от 23.07.1970 г. – *ДВ,* бр. 60 от 1970 г. В сила за България от 23.03.1976 г. Издаден от Министерството на външните работи. Обн. *ДВ,* бр. 43 от 28.05.1976 г.
2. **Микешин,** Л. А. Новая философская энциклопедия. В 4 тт. Под редакцией В. С. Стёпина. Москва: Мысль, 2001.
3. **Речник** на съвременния български книжовен език. [онлайн]. *https://ibl.bas.bg/rbe/lang/bg/.*
4. **Bentham,** J. Deontology, or The Science of Morality. 1834. [online]. *https://books.google.bg/books?id=hoaXYPKFt6cC&printsec=frontcover&hl=bg&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.*
5. **Vigouroux,** Christian, Déontologie des fonctions publiques. Dalloz, 2006.

ПЕРСПЕКТИВИ ЗА РЕСТАРТ НА ОТНОШЕНИЯТА ЕС – АФРИКА В СФЕРАТА НА РАЗУЗНАВАНЕТО И СИГУРНОСТТА

гл. ас. д-р Ангел Апостолов
Военна академия „Георги С. Раковски“

PROSPECTS FOR RESETTING EU – AFRICA RELATIONS IN THE INTELLIGENCE AND SECURITY FIELDS

Chief Ass. Angel Apostolov, PhD
Rakovski National Defense College

Резюме: *През последните пет години (2020 – 2023) вълната от преврати в африканските държави постави под въпрос способността на ЕС да комбинира ролята си на икономическа и политическа сила с тази на гарант на сигурността в разгара на съревнованието за геополитическо влияние между водещите центрове на сила. Въпреки че съществува реална необходимост от рестарт на отношенията ЕС – Африка в сферата на разузнаването и сигурността, все още липсва ясно определена рамка как подобна инициатива би могла да бъде осъществена най-оптимално. На първо място, следва да се отдаде приоритет на разузнавателния обмен между самите европейски държави в рамките на ЕС, а след това да се постигне по-оперативно ниво на сътрудничеството с разузнавателните служби на партньорските държави от Африка. На следващо място, е необходимо щателно преразглеждане на ОПСО по отношение на сътрудничеството с африканските държави за справяне с проблемите за сигурност в Африка.*
Ключови думи: *ЕС; Африка; Сахел; ОПСО; INTCEN; многостранно сътрудничество*

Abstract: *Over the past five years (2020 – 2023), the wave of coups in African countries has called into question the EU's ability to combine its role as an economic and political power with that of a security guarantor in the midst of competition for geopolitical influence between the major centers of power. Although there is a real need to restart EU – Africa relations in the field of intelligence and security, there is still no clearly defined framework for how the Union could implement such an initiative most efficiently. First, priority should be given to intelligence exchange between Member States within the EU itself, followed by achieving more operational level of cooperation with the intelligence services of partner countries in Africa. Next, in order to address the security challenges in Africa we need a thorough review of the CSDP policy regarding cooperation with the African countries.*
Key words: *EU; Africa; Sahel; CSDP; INTCEN; multilateral cooperation*

През последните пет години международният ред беше нарушен от няколко големи предизвикателства пред сигурността: пандемията от COVID-19, руската инвазия в Украйна през 2022 г., началото на войната на Израел срещу „Хамас“ през 2023 г. и вълната от преврати в африканските държави (2020 – 2023), където ЕС инвестира значителни ресурси, разположи персонал и в по-широк план се опита да утвърди ролята си на глобален фактор в областта на сигурността в продължение на повече от десетилетие. За разлика от първите три кризи, в които ЕС поддържа относително единна политика (с няколко ярки изключения по отношение на войната в Украйна), неотдавнашната вълна от преврати в държавите от региона на Сахел (вследствие получил названието „пояс на държавните преврати“), европейските държави все още не успяват да намерят единна политика с ясно изразен план и приоритети.

Това провокира въпроси относно водещата роля на Франция в ЕС по отношение на Африка, както и фундаментални въпроси за това как да се комбинира ролята

на ЕС на икономическа и политическа сила с тази на гарант на сигурността в разгара на съревнованието за геополитическо влияние между водещите центрове на сила. Решението на хунтата в Нигер внезапно да прекрати мисиите на ОПСО в страната добавя допълнителни въпроси относно бъдещата роля на ЕС в региона и като играч в сферата на сигурността в по-широк план [6: 1].

Сътрудничество в сферата на сигурността

Неотдавна Парламентарната комисия за сигурност на Италианската република (COPASIR) публикува доклад, който подчертава стратегическото значение на Африка за европейската сигурност и основните предизвикателства, пред които тя ще бъде изправена, ако ЕС цялостно не преосмисли политиката си по отношение на африканските държави – от Средиземноморието до Субсахарска Африка.

Документът призовава за създаване на специална институция на ЕС, координираща политиките за Африка, като подчертава необходимостта от „цялостна европейска стратегия за справяне с предизвикателствата, свързани с икономиката, сигурността и миграцията, основана на равното достойнство с африканските нации и подкрепена от необходимата решителност, ресурси и инструменти“ [2]. Някои от приоритетните области според документа са:

- **Противодействие на дезинформацията** – COPASIR предупреждава за нарастващи кампании за дезинформация от външни участници, особено от Русия и Китай, които използват пропаганда, за да подхранват антиевропейски настроения сред населението в африканските държави. Докладът призовава за координиран отговор на Запада за противодействие на тези разкази и за насърчаване на прозрачността в партньорствата с африканските нации.

- Комитетът също така подчертава необходимостта от по-големи усилия за увеличаване на дигиталната грамотност в Африка, където социалните медии се превърнаха в доминиращ източник на (дез-)информация за по-младите поколения – например платформи, като забранената в ЕС, но широкодостъпна в Африка Sputnik.

- **Предизвикателствата с миграцията** – COPASIR изчислява, че около 700 000 незаконни мигранти в момента са в Либия, повечето от които се готвят да заминат за Европа.

- Докладът подчертава критичната роля на сътрудничеството между разузнавателните служби на европейските и северноафриканските държави за разбиването на мрежите за трафик на хора. Макар че някои партньорства са ефективни, други са изправени пред значителни предизвикателства поради политическа нестабилност. Документът също така посочва връзките между организираната престъпност и терористичните групи, които използват миграционните маршрути за финансова печалба.

- Не на последно място докладът подчертава, че укрепването на граничната сигурност и международното сътрудничество между Европа и Африка трябва да остане основен приоритет.

Въпреки че съществува реална необходимост от рестарт на отношенията ЕС – Африка в сферата на разузнаването и сигурността, все още липса ясно определена рамка как подобна инициатива би могла да бъде осъществена най-оптимално. На първо място следва да се отдаде приоритет на развитието на сферата на сигурността, и в частност усъвършенстването на разузнавателния обмен между самите европейски държави в рамките на ЕС, а след това да се постигне по-оперативно ниво на сътрудничеството с разузнавателните служби на партньорските държави от Африка.

Възможно ядро на нова, щателно реформирана и разширена служба за разузнаване и сигурност на ЕС би могъл да изиграе Европейският разузнавателен и ситуационен център (EU INTCEN). EU INTCEN е създаден в рамките на Европейската политика за сигурност и отбрана в началото на XXI в. под името Съвместен ситуационен център. През 2002 г. Съвместният ситуационен център става форум за обмен на чувствителна информация между външните разузнавателни служби на Франция, Германия, Италия, Холандия, Испания, Швеция и Обединеното кралство. От 2011 г. EU INTCEN става част от Европейската служба за външна дейност (ЕСВД) под ръководството на Върховния представител на ЕС за външните работи и политиката на сигурност. Към 2025 г. Разузнавателният център се състои от два отдела:

- Аналитичен, който отговаря за изготвянето на стратегически анализи посредством материали, предоставени от разузнавателните служби на държавите членки;
- Поддръжка и разузнаване от открити източници [3].

EU INTCEN предоставя разузнавателна информация и анализи за целите на Общата външна политика и политиката за сигурност на ЕС (ОПСО), но действа и в областта на контратерористичната политика на Съюза. INTCEN и Дирекцията по разузнаване на Европейските въоръжени сили (Intelligence Directorate/ EUMS) са основните клиенти на Сателитния център на ЕС (EU SatCen), който им предоставя анализирана сателитна информация. INTCEN и Разузнавателният отдел на въоръжените сили на ЕС (Intelligence division of the EU military staff – INTDIR) изготвят доклади за нуждите на Комитета по отбрана (Military Committee) и на някои структури на ЕСВД, като съдържащата се в тях информация има предимно военен характер. Като първа стъпка към всеобхватна реформа на INTCEN би било създаването на специализирани отдели, например за ситуационен анализ и управление на кризи (в миналото INTCEN е имал подобни структури). На следващо място INTCEN може да бъде разширен, като структурата му получи обособяване по региони, подобно на самата ЕСВД*, където да се обръща особено внимание на специфичните проблеми в противодействието на предизвикателства към сигурността по региони и държави от особен интерес и повишен риск (каквито в Африка са например Сомалия и държавите от Сахел, както и граничещите с тях).

На следващо място необходимо е щателно преразглеждане на политиката ОПСО по отношение на сътрудничеството с африканските държави за справяне с проблемите за сигурност в Африка. Основна задача на дейността на ОПСО е да допринася за укрепване на демокрацията в рамките на по-широки усилия за изграждане на мира. Въпреки това свързаните с управлението елементи на мисиите и операциите по ОПСО, включително тези, които са свързани с изграждането на стабилни демократични структури, с времето намаляват в полза на по-тясно дефинирано, прагматично сътрудничество в областта на сигурността. Руското нахлуване в Украйна през 2022 г. до известна степен възроди връзката между изграждането на способности в сферата на сигурността редом до стабилни и работещи демократични институции, особено в Източна Европа, но не в еднаква степен във всички места, където действа ОПСО, като основен дефицит в изграждането на демократични ценности се наблюдава в Африка [4].

Глобалната стратегия на ЕС от 2016 г. подчертава „принципния прагматизъм“ и през тази година Съветът на ЕС предложи преразглеждане на гражданските мисии по ОПСО „в светлината на променящите се политически приоритети“. Държавите – членки на ЕС, като цяло се колебаят да осигурят персонал, като експерти по върховенството на закона и съдии в мисиите на ОПСО. Амбицията на ОПСО за обхвата на

* Шест големи отдела на ЕСВД обхващат всички региони по света – Африка, Северна и Южна Америка, Азия и Тихоокеански регион, Европа, Източна Европа и Централна Азия, Близкия изток и Северна Африка. Друг отдел е посветен на Глобалния дневен ред и многостранните отношения.

нейните мисии и операции се стеснява, тъй като подкрепата за прокарване на демократични реформи в Африка намалява и се сблъсква с нарастващото геополитическо съперничество за влияние. ОПСО започва да се съсредоточава предимно върху помалки мисии, с ограничен мащаб и насочени към реформа на сектора за сигурност, както и върху мисии за мониторинг, с участие на съветници, обикновено с ограничено ресурсно обезпечаване.

От всички мисии на ОПСО, създадени от 2003 г. насам, огромното мнозинство са били в Африка, на юг от Сахара, където опитът на ЕС разкрива по-милитаризиран и деполитизиран подход. Например от мисията на ЕС за изграждане на способности (EUCAP) Sahel Niger и EUCAP Sahel Mali обещаха да рационализират върховенството на закона чрез по-скромна консултативна роля, фокусирана главно върху силите за сигурност на всяка държава. През 2015 г. военната мисия на ЕС за обучение (EUTM) в Мали – най-голямата по рода си – и двете EUCAP бяха „адаптирани към политическите приоритети на ЕС, по-специално след мобилизацията на ЕС срещу незаконната миграция и свързания с нея трафик“ [4].

Въпреки че през 2023 г. доклад на Европейския парламент относно гражданската ОПСО призова за по-широко сътрудничество с приемащите държави за изпълнение на ангажиментите за институционална реформа и правата на човека, ЕС остава предпазлив относно включването на изрични препратки към целите на правата на човека в мандатите на ОПСО, особено в тези за военни операции, в които обикновено липсват експерти в тези области. Изпълнението на ангажиментите на ОПСО по отношение на правата на човека и демократичния надзор е слабо. По този начин до голяма степен се обезсилва основното предимство на мисиите и операциите на ОПСО в сравнение с участници като „Вагнер“ – не просто решаване на кризата в настоящия момент, но и изграждане на стабилни демократични институции, които да могат да се справят с възникване на подобни кризи в бъдеще – нещо, което частни военни компании като „Вагнер“ нямат нито капацитет, нито интерес да постигнат.

Изглежда сигурно, че ЕС ще продължи да развива ОПСО с фокус върху непосредствените интереси на Съюза и опасенията за сигурността. В ход са нови инициативи, като Капацитет за бързо развитие, който ще позволи на блока бързо да разположи мобилна бригада от до 5000 войници. През декември 2024 г. Съветът на ЕС препоръча ОПСО да задълбочи своите взаимодействия със съответните участници в ЕС за справяне с тероризма и въоръжения екстремизъм.

Ревизия на стратегията на ЕС за Африка

ЕС има потенциал да направи повече, за да съживи включването в ОПСО на въпроси, свързани с демократичното управление, по начин, който е в съответствие с реалната политика. Например ЕС би могъл да насърчи диалога между участниците в областта на демокрацията, мира и сигурността и да засили връзките между експерти и практици, включително на равнище разузнавателни органи. Съюзът би могъл да се съсредоточи повече върху предотвратяването на конфликти и мирното посредничество чрез подкрепа за отворени, безопасни пространства и приобщаващи плуралистични дискусии, като позволи работата на ОПСО в такива области.

В същото време Съюзът би могъл да гради върху въпроси, свързани с управлението, в обещаващи среди, като по този начин свързва прокарването на демократичните принципи с прагматичните цели. ЕС – и в частност ОПСО – биха могли също да разширят своята роля чрез свързване на тематични области и интегриране на своите граждански и военни измерения. Реформата и на общоевропейските органи за ра-

зузнаване и сигурност и прагматичното разширяване на обхвата на споделена информация с държавите – партньори от Африка, може да спомогне не само за стабилизиране на тези държави, но и за изграждане на трайно взаимно доверие. Геополитическите предизвикателства означават, че ЕС трябва да намери начини да възстанови ОПСО като значима част от своя инструментариум за подкрепа на демокрацията.

С подходящите рамки и стандарти Африка и Европа могат да изградят дълготрайно и многоизмерно партньорство в редица области – политика, сигурност, икономика, човешки ресурси и др. Но усилията за максимизиране на ползите от такова партньорство изискват промени и от двете страни. Европа традиционно вижда своята роля на международната сцена по три начина: тя е световна търговска сила и доставчик на помощ за развитие; участник в политиката и сигурността, подкрепящ регионалната сигурност чрез органи като АС; и нормативна власт, подкрепяща правата на човека и демокрацията, регионалната интеграция и многостранните организации [1].

В свят на нарастваща геополитическа конкуренция, с транснационални въпроси, като изменението на климата, миграцията и технологиите, които заемат важна роля, Европа трябва да се фокусира върху няколко приоритетни области на действие. Такива биха могли да бъдат:

- всеобхватни и проактивни подходи за сигурност;
- укрепване на местните партньорства и изграждане на способности;
- адаптиране към асиметрични заплахи за сигурността;
- интегриране на връзката климатични промени – енергиен преход;
- подобряване на многостранното сътрудничество между ЕС и Африканския съюз;
- отговор на миграционни и хуманитарни кризи;
- противодействие на хибридните заплахи;
- технологична и цифрова адаптация;
- гъвкаво, бързо разгръщане и реакция при кризи;
- акцент върху правата на човека, демокрацията и върховенство на закона.

Мисиите на ОПСО следва да продължат да играят основна роля в подкрепа на създаването на отчетни и прозрачни институции, да се възползват от по-добрата координация с тези организации, за да се избегне дублирането на усилията и да се повиши ефективността на поддържането на мира и разрешаването на конфликти.

Заключение

Тъй като глобалните предизвикателства стават все по-сложни, мисиите и операциите на ЕС по ОПСО трябва да се развиват, за да останат важно и ефективно средство за поддържане на международния мир и сигурност, особено в Африка.

Африканските държави търсят по-голяма степен на свобода за установяване на отношения, които биха могли да бъдат от полза за тях, с нови партньори, които преди това не са присъствали в Африка – по-специално с Китай заради неговия търговски и инвестиционен потенциал, а също и с Русия за тези, които искат да се снабдят с оръжие и подкрепа на въоръжени наемници. В действителност обаче никоя от тези алтернативи не предлага същите предимства като Европейския съюз, който остава водещият търговски партньор, водещият доставчик на продуктивни преки инвестиции, които генерират заетост, и партньорът, който може да им предложи сътрудничество, което да ги интегрира по-изгодно и по стабилен начин с частта от света, която е най-допълваща за тях в глобалния контекст [5: 63].

Чрез засилване на способностите си за бързо реагиране и поддържане на силен акцент върху правата на човека и управлението ЕС може да гарантира, че неговите

мисии допринасят значително за дългосрочния мир и стабилност в региони, като Южното Средиземноморие и Субсахарска Африка.

Литература

1. **Balfour,** R., L. Bomassi, M. Martinelli. (2022). The Southern Mirror: Reflections on Europe from the Global South. – In: *Carnegie* Endowment for International Peace. [online]. [available 9.04.2025]. *https://carnegieeurope.eu/2022/06/29/southern-mirror-reflections-on-europe-from-global-south-pub-87306*.
2. **Covato,** V., F. Vincenzoni, L. Bader, E. Comin. (2025). Italy's intel committee calls for EU strategy on Africa. – In: *Decode39.* [online]. [available 9.04.2025]. *https://decode39.com/9905/italy-s-intel-committee-calls-for-eu-strategy-on-africa/*.
3. **European** Union External Action Service – Structure and Organization. [online]. [available 9.04.2025]. *https://www.eeas.europa.eu/eeas/structure-and-organisation_en*.
4. **Farinha,** Ed. (2025). The EU Common Security and Defense Policy: Moving Away From Democracy Support. – In: *Carnegie* Europe. [online]. [available 9.04.2025]. *https://carnegieendowment.org/research/2025/03/the-eu-common-security-and-defense-policy-moving-away-from-democracy-support?lang=en*.
5. **Florensa,** S. (2024). Beyond the Neighbourhood: Africa and Europe in the New Global Geopolitical Order. – In: *IEMed* Mediterranean Yearbook 2024. [online]. [available 9.04.2025]. *https://www.iemed.org/med-yearbook/iemed-mediterranean-yearbook-2024/*.
6. **Wilén,** N. (2023). Have African Coups provoked an Identity Crisis for the EU? – In: *Egmont* Policy Brief 323. [online]. [available 9.04.2025]. *https://www.egmontinstitute.be/app/uploads/2023/12/Nina-Wilen_Policy_Brief_323_vFinal2.pdf*.

БИЗНЕС РАЗУЗНАВАНЕ И НЕЛОЯЛНА КОНКУРЕНЦИЯ

д-р Костадин Язов
Висше училище по сигурност и икономика – Пловдив

BUSINESS INTELLIGENCE AND UNFAIR COMPETITION

Kostadin Yazov, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Бизнес разузнаването включва икономически, промишлен, търговски, научно-технически шпионаж, означава активни действия, насочени към събиране, натрупване и обработка на ценна информация, забранена за достъп на трети лица. Бизнес разузнаването е легално и етично разузнаване въз основа на открити източници за макро- и микрообкръжението, при което явленията и тенденциите се разглеждат от гледна точка на конкуренцията и конкурентната борба; то изключва използването на оперативните методи и не се явява промишлен шпионаж. Много често бизнес разузнаването носи информация, която се използва за действия, нарушаващи добросъвестната търговска практика, и това е формулирано в Закона за защита на конкуренцията като нелоялна конкуренция и може да увреди интересите на конкурентите.*

Ключови думи: *бизнес разузнаване; търговско разузнаване; конкурентно разузнаване; информационно разузнаване; организация; нелоялна конкуренция*

Abstract: *Business intelligence includes economic, industrial, commercial, scientific and technical espionage, it means active actions aimed at collecting, accumulating and processing valuable information, prohibited for access by third parties. Business intelligence is legal and ethical intelligence based on open sources for the macro- and microenvironment, in which phenomena and trends are considered from the point of view of competition and competitive struggle, it excludes the use of operational methods and is not industrial espionage. Very often, business intelligence carries information that is used for actions that violate fair trade practice and this is formulated in the Law on Protection of Competition as unfair competition and can damage the interests of competitors.*

Key words: *business intelligence; commersial intelligence; competetive intelligence; information warfare; organization; unfair competition*

Същност на бизнес разузнаването

В съвременната епоха мащабите на икономическия шпионаж рязко нарастват и за тази цел се харчат много финансови ресурси. Информацията за интелектуалната собственост, за резултатите от чуждите приложни и фундаментални изследвания позволява да се икономисат собствени сили и средства и да се съсредоточи цялото внимание върху производството и маркетинга. По-нататъшното развитие на научно-техническия прогрес, увеличаването на потока на патентите и ожесточаването на конкуренцията като „война на всички против всички“ правят присвояването на чуждите секрети особено печелившо и затова привлекателно.

Икономически разузнавателни данни днес се събират чрез най-различни методи, като много от тях не са съвсем надеждни по истинност, но всички имат някаква ефективност по принцип.

Конкуренцията открива пътя към развитието на едни и към унищожаването на други, но това означава прогрес. Тя поставя противниците в такива тежки условия, че

те са принудени да участват в играта без правила и да постъпват по принципа „победителите не ги съдят“. Конкуренцията е борба в името на победата. Побеждава този, който може по-добре, по-качествено и по-евтино да организира производството на стоки и предоставянето на услуги. Това провокира съперниците непрекъснато и неуморно да търсят нови пътища за увеличаване на доходите, което води до по-нататъшното развитие на прогреса. Победителят получава винаги повече, отколкото победения и това е универсално правило. В икономическата конкуренция победата трябва да бъде всекидневна. В конкурентната борба не може да има вечни победители. Свидетели сме на глобална хиперконкуренция и лесно навлизане на чужди фирми на нашите местни пазари и трудно излизане на нашата стока на външни европейски пазари.

Бизнес разузнаването е претърпяло развитие и еволюция през годините. Отначало на него са възлагали задачи по оценка на потребностите от необходима информация, както и на нейното планиране, събиране, анализ и презентация. По-нататък към тях се добавят прилагане на резултатите от разузнаването, защита и натрупване на опит. Върху бизнес разузнаването и неговото институционализиране оказват съществено влияние глобализацията, разпространението на информационните технологии и огромната потребност от достоверни резултати. Действията по събирането и обработката на информацията [5: 99] дават възможност да се получи не само информация за вземане на съответните решения, но и данни, които могат да се използват за оценка на резултатите от дейността на бизнес разузнаването.

Една от най-важните цели на конкурентното разузнаване е съкращаването на времето, необходимо за подготовка на отговорите на ситуативните искания при нарастване на степента на участие в работата на „екипите“, готвещи и взимащи решения. Най-добре е да се използва комбинацията с неявни и косвени методи за получаване на сведения, тъй като в този случай може да се получи по-дълбоко разбиране на изследвания проблем и по-достоверни резултати. Резултатите, получени с прилагането на аналитични методи и схеми, се приемат като обективни.

Аналитичната информация може да се разпространява в електронна форма, в хартиен вариант, да се съобщава устно или да се записва. Такова „излишество“ е пример за внимание към потребителите на информацията, тъй като предпочитанията относно носителите на информация варират. При това е необходима ефективна комуникация, за да достигнат резултатите от анализа до потребителя. Ако не са ефективно доведени резултатите от анализа до ползвателите на информацията, не може да се спечели тяхното доверие, тъй като ползвателите са основната движеща сила на конкурентното разузнаване. На свой ред е важно да се определи в каква степен и в кои етапи мениджърите ще бъдат въвлечени в корпоративното разузнаване. Мениджърите са длъжни да определят потребностите от информация и да осигуряват обратна връзка в течение на целия проект. Реализацията на препоръките, формулирани в резултат на анализа на информацията, остава задължение на мениджърите на производствените, маркетинговите и другите функционални отдели. След това е важно да се съсредоточи вниманието върху получаването и анализа на сведенията, за да се разработят и своевременно да се обновят масивите от информация за дейността на конкурентите.

Еволюцията на програмите на бизнес разузнаването трябва да се приеме като естествен процес, идентифициращ потребностите на организацията, обратната връзка и мероприятията за повишаване на качеството на конкурентното разузнаване.

Методи и източници за събиране на информация

Могат да се диференцират два вида бизнес разузнаване – стратегическо и оперативно. Задачите на стратегическото бизнес разузнаване плътно се доближават до

задачите на стратегическото планиране и маркетинг и се свеждат до изясняване на структурата и динамиката в полето на стопанско-икономическата дейност, на което работи или се готви да работи организацията, с определяне и анализ на всички конкуренти и контрагенти. Оперативното бизнес разузнаване решава непосредствените задачи по работата с конкретния конкурент и често действа на границата на етичните и правно приемливи норми и средства.

Акцентът на работата се поставя върху търсенето и откриването на слабите места на фирмата конкурент. За да се спечели схватката с конкуренцията, е необходимо да се разбира организацията конкурент. През 500 г. до н.е. гениалният китайски стратег Сун Дзъ написва книгата „Изкуството на войната“. В нея той подчертава следното: „Ако вие не познавате себе си и своя враг, то вие сте глупак и несъмнено ще претърпявате поражение във всяка една битка. Ако вие познавате себе си, но не познавате своя враг, то веднъж ще победите, веднъж ще загубите. Ако вие познавате себе си и своя враг, то ще побеждавате във всяко едно сражение“.

Нуждата от информация за конкурентите като че ли автоматически поставя въпроса за корпоративната сигурност. Често пъти тази дейност се оказва неефективна поради това, че при формулирането на задачите не е фокусирана върху крайната цел на организацията. В резултат на такъв подход се натрупва голям обем факти и данни, които, макар и интересни, в необработен вид не представляват особено голяма ценност при вземането на стратегически и тактически управленски решения.

В основата на системата на бизнес разузнаване лежи цикълът на разузнаването, в резултат на който „суровата“ необработена информация се превръща в разузнавателни сведения – база за взимане на управленски решения.

Бизнес разузнаването дава най-добри резултати, ако е организирано като непрекъснат процес. При организацията на широкомащабна система за разузнаване от собствената организация е необходимо стремежът да бъде към разширяване на сферата на дейност извън пределите на организацията и привличане на колкото се може повече сътрудници. Успешно работещите организации разглеждат конкурентното разузнаване като важно задължение на лицата от висшата администрация и активно участие и съпричастност на целия персонал. Ограничаването на достъпа до информацията на конкурентното разузнаване само за ръководителите на най-високо ниво води до „забравяне“ на специалистите. Те също би трябвало да получат информация от конкурентното разузнаване и да я използват в своята работа. Нещо повече, ограничавайки достъпа на някои специалисти до визираната информация, у някои от тях може да изчезне желанието да предоставят в организационната система за разузнаване събраните от тях данни.

Използване на достъпна информация от открити източници (OSINT)

„OSINT“ („Open Source INTelligence“) е термин, означаващ събиране и анализ на разузнавателни данни на основата на информация от общодостъпни източници. Според достоверни оценки основните разузнавателни централи по света вече получават своите данни до 95 на сто от открити източници, като разходите за тях са само 1 на сто от разузнавателните бюджети. Настъпва ерата на професионалния аналитичен шпионаж, т.е. анализът на вестници, интернет, книги, телефонни справочници, научни списания, радиопредавания, правителствени отчети, техническа документация, инструкции и т.н.

От гледна точка на разузнаването OSINT [1: 23] принципно се различава от „простата“ информация (наричана „OSIF“, или „Open Source Information“), т.е. въобще някакви данни и сведения, циркулиращи по всички достъпни медии и канали.

OSINT никога не е „въобще“, а винаги е специфична информация, събирана и структурирана за отговор на конкретни въпроси.

Събирането на разузнавателни данни OSINT се различава от другите направления на разузнавателната дейност, преди всичко от HUMINT, т.е. агентурното разузнаване. В OSINT главният проблем е търсенето на надеждни източници сред огромното изобилие на общодостъпна информация. Ако бъдат намерени тези източници, получаването от тях на разузнавателни данни не е трудно.

Деленето на разузнаването на „открито“ и „тайно“ е условно. Значителна част от агентурното разузнаване се свежда до получаването на информация от знаещи хора, заради което също може да се счита за част от OSINT. Разузнавателните данни от открити източници не само се отличават от секретните, но и нерядко ги превъзхождат със своята точност. На първо място, е оперативността при анализа на откритите източници. Когато в някоя точка на планетата започва криза, възможностите за разузнаване там не са големи. Структурите, формиращи политиката на държавите, и аналитиците на разузнавателните служби включват телевизори и се впускат в интернет. На второ място, е обемът на получаваната информация. В света има много повече свободни анализатори, журналисти, независими експерти и други осведомени хора от кадровите разузнавачи. Както показва опитът, грамотно събраната информация от открити източници е много по-значима от секретните разузнавателни отчети. На трето място, е качеството. Надеждността на откритите източници може да е ясна или неясна, но при получената тайно информация степента на достоверност е винаги неясна и спорна.

Вече се счита, че OSINT е най-перспективният метод на разузнаване. Но методите на OSINT могат да са ефективни само когато крайните потребители на данни се интересуват от реалното състояние на нещата, а не от политическата конюнктура. Ако в спецслужбите действат тайни структури, които се занимават с криминални операции извън законите, за тях OSINT също е сериозен проблем, тъй като ги разобличава. Именно заради това не получава водеща роля в спецслужбите на САЩ, Англия и Израел. Това обаче не намалява важността и актуалността на OSINT.

Същност на нелоялната конкуренция

През последните години проблемът за нелоялната конкуренция присъства в стопанската дейност на почти всички фирми, а нейните последици са особено неблагоприятни за тяхното развитие. Без наличието на конкуренция стопанството не би могло да функционира нормално, но все по-често полезната конкуренция се превръща в нелоялна и в крайна сметка в пагубна.

Разумната конкуренция разпределя доходите в зависимост от пазарния успех, води до оптимална организация на производствения процес и търговията, преодолява пазарния дефицит, стимулира иновациите и научно-техническия прогрес. Чрез нея се поддържат ниски цени, високо качество и редуцирани разходи. Превръщането ѝ обаче в неразумна и нелоялна застрашава нормалните икономически отношения в обществото и унищожава с бързи темпове устоите на стопанската система.

Нелоялна конкуренция представлява всяко действие или бездействие при осъществяване на стопанска дейност, което е в противоречие с добросъвестната търговска практика и уврежда или може да увреди интересите на конкурентите в отношенията помежду им или в отношенията им с потребителите.

Проблемът, наречен „нелоялна конкуренция“, е в състояние да унищожи из основи дори най-стабилния и дългогодишен бизнес. Именно по тази причина при наличие дори на незначителна индикация за появата на подобен вид проблем застрашените лица следва незабавно да потърсят правна защита от компетентни професионалисти.

Нелоялна конкуренция по смисъла на Закона за защита на конкуренцията (ЗЗК) [4] може да е всяко действие или бездействие при осъществяване на стопанска дейност, което е в противоречие с добросъвестната търговска практика и увреждa или може да увреди интересите на конкурентите (чл. 29 от ЗЗК).

За да се установи нарушение по ЗЗК, е необходимо да са налице няколко задължителни условия.

Наличие на стопанска дейност и отношение на конкуренция между страните по преписката. Това изискване разграничава правомощията на Комисията за защита на конкуренцията (КЗК) от правомощията на Комисията за защита на потребителите. Докато Законът за защита на потребителите е насочен към пряка защита на основни права на потребителите (чл. 1 от ЗЗП), основната цел на ЗЗК е да осигури защита и условия за разширяване на конкуренцията и на свободната инициатива в стопанската дейност. Това на практика означава, че КЗК следи за чистотата на пазарните отношения между предприятията конкуренти, чрез което косвено защитава и крайните потребители.

ЗЗК посочва, че е без значение формата на предприятието (§ 1, т. 7 от ДР на ЗЗК), и по този начин предоставя защита на всички физически, юридически лица и неперсонифицирани образувания, които извършват стопанска дейност. Така, освен търговците по смисъла на Търговския закон, ЗЗК предоставя защита срещу нелоялни действия на всички други лица, чиято организирана дейност в предприятие определя тези лица като търговци. За да са налице отношения на конкуренция, страните трябва да извършват своята стопанска дейност на един и същ съответен пазар, а това е така, когато предлагат стоки или услуги, които могат да се приемат от потребителите като взаимнозаменяеми по отношение на техните характеристики, предназначение и цени, от една страна, и от друга – предлагат тези стоки или услуги в границите на една и съща територия.

Какво означава осъществяване на действие или бездействие, което е в противоречие с добросъвестната търговска практика? Противоречие с добросъвестната търговска практика е налице, когато с извършеното действие или чрез бездействие се нарушават писани (нормативни актове) или неписани (наложени между стопанските субекти обичайни търговски отношения или възприетите добри нрави) норми на поведение, свързани със съответната стопанска дейност.

Наличие на увреждане или на възможност за увреждане на интересите на конкурентите. Самото осъществяване на конкурентна дейност не се приема за увреждащо интересите на конкурентите. Действието или бездействието, противоречащо на добросъвестната търговска практика, трябва да увреждa реално интересите на конкурентите или най-малкото да създава възможност за такова увреждане.

Най-характерните и най-често срещаните форми на нелоялна конкуренция са посочени в специалните текстове на ЗЗК (чл. 30 – 37).

Установяване и пресичане на нелоялната конкуренция

Нелоялната конкуренция е изключително трудно доказуема. Възможно е даден мениджър да е напълно убеден, че неговото търговско предприятие е субект на нелоялна конкуренция, но за него да бъде абсолютно невъзможно да го докаже по официален ред. От друга страна на него страшно му се иска нелоялната конкуренция да бъде прекратена най-малко защото търпи от нея материални вреди и пропуснати ползи.

Изходът в този случай е мениджърът да възложи на структурата за сигурност да преустанови нелоялната конкуренция срещу фирмата. Тази дейност се осъществява в подсистемата на вътрешната сигурност [2: 83] чрез две групи способи – способи за прекратяване и способи за пресичане на нелоялна конкуренция.

Под „прекратяване на нелоялната конкуренция“ се разбират дейности, осъществявани от фирмения контрашпионаж на потърпевшото предприятие, които довеждат под страх от настъпване на вредоносни последици до прекратяване на нелоялната конкуренция от инициатора по собствена негова подбуда.

Вредните последици могат да бъдат най-различни. Тези последици обаче трябва наистина да са достатъчно страшни, че да уплашат не на шега нелоялния конкурент. Търговските му интереси трябва да са достатъчно силно засегнати или поне поставени в реална опасност. Тоест интензитетът на прекратяващото нелоялната конкуренция въздействие трябва да е достатъчно силен, за да мотивира отказа на нелоялния конкурент с висока вероятност. В крайна сметка прекратяването на нелоялна конкуренция идва като последица от управленското решение на мениджъра на инициралото я търговско предприятие. Ето защо най-резултативните способи от страна на структурата за сигурност на потърпевшия са свързани с реализирането на дейности, които оказват влияние върху управленския процес на нелоялния конкурент. Управленският процес на инициатора трябва да бъде саботиран, но по „благородни“ подбуди. Тук е възможно приложението на методи за въздействие върху волята на инициатора, за дезинформация, за принуда, за компрометиране и др.

Пресичането на нелоялна конкуренция не е в зависимост от волята на нейния инициатор. Той продължава да желае нейното продължаване, но поради независеща от него причина нелоялната конкуренция е била преустановена. Преустановяването трябва да е настъпило поради действия на структурата за сигурност на потърпевшия, иначе за никакво пресичане не може да става дума. Какви биха могли да бъдат тези действия? Те също са най-различни, в зависимост от конкретни обстоятелства. Например разкрито и отстранено е било довереното лице на нелоялния конкурент сред собствения персонал на потърпевшия, в резултат на което то повече не е в състояние да изнася конфиденциална информация. Или пък потърпевшият е изградил система за регистратура, която е преустановила нерегламентирания достъп на инициатора до конфиденциална информация, и др.

Бизнес разузнаване и сигурност на фирмата

Всяко дружество е принудено да работи в условия на глобална несигурност, в голяма степен на непосредствена, тактическа несигурност. В атмосферата на констатирана ожесточена икономическа и технологична конкуренция все повече дружества са подтикнати, склонни, принудени да набавят липсващата им информация чрез методите на бизнес разузнаването. Когато те се управляват лошо и това се съчетае с егоизма на човека, служителя, се създават идеални условия за предателство и шпионаж.

Човекът е най-слабото звено в системата за фирмена сигурност, тъй като служителят е най-големият източник на информация, той създава информация, работи с информация, създадена от колегите му, и съобразно естеството на функционалните си задължения разпространява информация. Вследствие на двойствената социалнопсихологическа характеристика на човека служител той може да бъде лоялен или нелоялен към интересите на фирмата.

Следователно произтичат две взаимносвързани задачи. Едната задача е да се придобива информация за конкурента, партньора и клиента, включително и с методите и средствата на бизнес разузнаването. Другата важна задача е да се защити сигурността от действията на бизнес разузнаването на конкурента, партньора, клиента, криминалния свят и специализираните фирми за разузнавателни услуги.

Богатият международен опит показва, че нито едно, било то физическо, или юридическо лице не може ефективно да действа в условията на остра конкурентна

борба без задълбочено и всестранно разбиране за състоянието на пазарната среда или без да разполага с нова, пълноценна и достоверна информация за протичащите в нея процеси. В тази връзка динамично се развива бизнес разузнаването или business intelligence – (BI), както и понятията „търговско разузнаване“ („Commersial Intelligence“), „конкурентно разузнаване“ („Competetive Intelligence“), „индустриален (корпоративен, икономически) шпионаж“ („Industrial (Corporate) Espionage“), „информационно разузнаване“ („Information Warfare“), „фирмено (корпоративно) разузнаване“, „икономическо разузнаване“, „стопанско разузнаване“, „маркетингово разузнаване“ („Marketing Intelligence“), „банково разузнаване“.

„Бизнес разузнаване“ е събиране и обработка на данни от различни източници, осъществяващо се в рамките на закона и при спазване на етическите норми, за разлика от промишления шпионаж, подпомагащи изработването и взимането на ефективни управленски решения с цел повишаване на конкурентоспособността на бизнес организацията. Бизнес разузнаването повишава ефективността на бизнеса чрез изработването и взимането на ефективни управленски решения както на стратегическо, така и на тактическо ниво. Изпълнява функциите на система за „ранно предупреждение“, привличайки вниманието на мениджърите на възможно най-ранен етап към заплахите, които потенциално могат да причинят щети на бизнеса на фирмата.

Заключение

Бизнес разузнаването установява благоприятните за бизнеса възможности, които е желателно да не се пропускат и които фирмата би могла просто да не забележи, ако не използва възможностите на бизнес разузнаването. Съдейства на структурата за сигурност на фирмата, участвайки в установяването на опити от страна на конкурентите да получат достъп до фирмените секрети. Изпълнява функциите на механизъм за управление на рисковете, което позволява на компанията ефективно да реагира на бързите изменения в околната среда.

Бизнес разузнаването създава във фирмата чувство за сигурност, осъзнатост за това, че съдбата на фирмата се намира в нейните собствени ръце и че тя няма да стане внезапна жертва на обстоятелства или някакви враждебни действия.

Изхождайки от реалностите на съвременното общество на серийно произвеждани несигурности, е особено актуален въпросът за същността, ролята и значението на бизнес разузнаването в глобалната икономика.

Литература

1. **Василев,** В. Разузнаване без тайни. – В: *Строго* секретно, бр. 143, с. 23, OSINT.
2. **Григоров,** В. Основи на фирмената сигурност. Велико Търново: Касиопея, 2002.
3. **Етичен** кодекс. Българска асоциация „Корпоративна сигурност“ (БАКС). [онлайн]. *https://bacsbg.com/documents/.*
4. **Закон** за защита на конкуренцията. [онлайн]. *https://lex.bg/bg/laws/ldoc/2135607845.*
5. **Мичев,** С. Сигурността в информационното общество. София: Софттрейд, 2004.
6. **Сёмин,** Н. Л. Спецслужбы и крупный бизнес США. [онлайн]. *warandpeace.ru.*
7. **Briody,** D. The Iron Triangle. Inside the Secret World of the Carlyle Group. New Jersey: John Wiley & Sons Inc, 2004.
8. **Perry,** David L. Business Intelligence and National Intelligence: Should the CIA Spy for American Companies? Davenport College/Smiths Industries Distinguished Visitor, 1993. (From a speech given on 15 February 1993 at Central Reformed Church, Grand Rapids, Michigan.)
9. **Smith,** Michael. Private Intelligence Companies – How the Spooks Moved in on Big Business.
10. **The** Iron Triangle. Inside the Secret World of the Carlyle Group, p. 120. – In: *Weekly* Standard, January 29, 2007.

БЛОКЧЕЙН В РАЗУЗНАВАНЕТО

д-р Теодора Личева
Нов български университет – София

BLOCKCHAIN IN INTELLIGENCE

Teodora Licheva, PhD
New Bulgarian University – Sofia

Резюме: *Непрекъснато развиващите се информационни технологии поставят нови предизвикателства и изисквания пред разузнавателните служби. Един от най-иновативните подходи е използването на блокчейн технологии – система, която осигурява защита, прозрачност и проследимост на данни чрез децентрализирана архитектура. В международен план държавите се стремят да интегрират съвременни технологии, за да осигурят надеждност на данните и интегритет при обмена на информация между различни структури и организации.*
Ключови думи: *разузнаване; блокчейн; киберсигурност; данни*

Abstract: *The continuously evolving information technologies present new challenges and demands for intelligence services. One of the most innovative approaches is the utilization of blockchain technology – a system that ensures data security, transparency, and traceability through a decentralized architecture. At an international level, countries are striving to integrate modern technologies to ensure data reliability and integrity during the exchange of information between various structures and organizations.*
Key words: *intelligence; blockchain; cybersecurity; data*

Увод

В съвременната динамична среда за сигурност разузнавателните служби са изправени пред нарастващи предизвикателства, свързани със събирането, обработката, съхранението и защитата на информацията, включително и на чувствителната. Блокчейн технологията, първоначално създадена като основа за криптовалутите, демонстрира значителен потенциал за трансформиране на разузнавателната дейност чрез своите уникални характеристики на децентрализация, прозрачност и непроменимост на записаните данни във веригата. Настоящото изследване анализира възможностите за интегриране на блокчейн технологиите в разузнавателната дейност, като се фокусира върху:

- правната рамка в България;
- конкретни приложения и бъдещи ползи;
- международния опит и добри практики и сравнителен анализ – Съединени американски щати (САЩ), Китай и Франция.

Разузнаване

Разузнаването е процес на събиране, анализ и използване на информация, която има стратегическо значение за националната сигурност. Основните цели включват:

- **Събиране на надеждна информация:** идентифициране и анализ на заплахи и рискове за националната сигурност.
- **Предотвратяване на терористични дейности и кибератаки:** чрез ранно предупреждение и предотвратяване на заплахите в реално време.

▪ **Подпомагане на политическите и военните решения:** чрез предоставяне на обективна и детайлна информация за вземане на информирани навременни решения.

За да бъдат успешни, разузнавателните служби трябва да разполагат с висококачествени, навременни и точни данни, като всяка малка грешка или манипулация може да има сериозни и необратими последици [9].

Съгласно Закона за управление и функциониране на системата за защита на националната сигурност [1] на Република България разузнавателните служби имат право да използват съвременни технологични решения за изпълнение на своите функции при спазване на строги изисквания за защита на информацията. Ключови аспекти от закона, релевантни към използването на блокчейн:

▪ Чл. 3 определя принципите на законност, обективност и политически неутралитет;

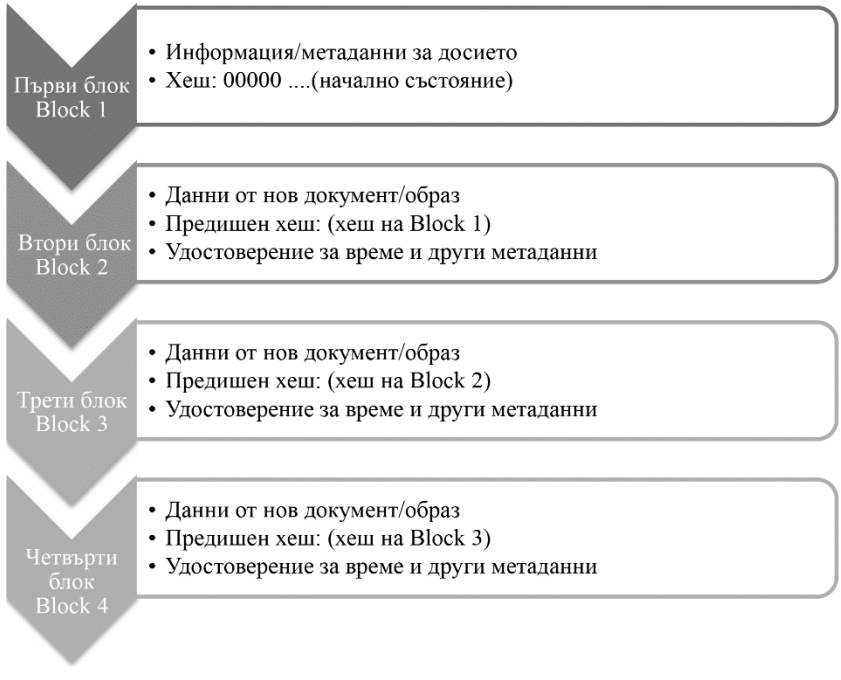
▪ Чл. 4 регламентира координацията между различните служби;

▪ Чл. 8 касае информационното осигуряване и защитата на информацията.

Основна характеристика на блокчейн

Блокчейн е децентрализирана и непроменяща се цифрова книга, която съхранява данни чрез последователно свързани блокове. Всеки блок съдържа криптографски подпис (хеш), който гарантира автентичността и целостта на записаната информация. Основните принципи включват децентрализация, прозрачност, сигурност чрез криптография и консенсусни алгоритми, които предпазват от неоторизирана манипулация [2: 141 – 148].

Фигура 1. ***Схематично представяне на технологията блокчейн***



Първоначално блокчейн технологията стана известна с появата на криптовалутата биткойн, но с течение на времето нейното приложение се разширява и извън сферата на финансите. Сегашните приложения включват електронно управление на данни, проследяване на веригата на доставки, здравеопазване и, разбира се, създаване на електронни досиета [3: 127 – 137]. Тази еволюция е продиктувана от нуждата за подобрена сигурност и намаляване на зависимостта от централно управлявани системи.

Възможности на блокчейн в разузнаването

Фигура 2. ***Използване на блоковата верига в разузнавателните процеси***

Внедряването и използването на блокчейн в разузнаването е нова възможност, която съчетава традиционните методи на събиране и анализ на данни с модерни технологии за сигурност. Целта е да се използват децентрализирани бази данни, които гарантират, че информацията не може да бъде променяна или манипулирана от неавторизирани лица [17]. Това позволява на разузнавателните структури да се възползват от предимствата на блокчейн за криптографска защита, прозрачност на веригата на данни, проследимост и времевия отпечатък върху на операциите.

Международен опит за използване на блокчейн в разузнавателните структури

Съединени американски щати

Агенциите от разузнавателната общност на САЩ интензивно използват и експериментират с блокчейн технологии, като имат създадени специализирани агенции, като:

- DARPA[1] разработва защитени комуникационни платформи;
- NSA[2] изследва приложения за криптографска защита;
- CIA[3] инвестира в блокчейн стартъпи чрез In-Q-Tel [13].

Проучване, публикувано в IEEE Access [14], представи анализ на внедряването на блокчейн технологии в области на сигурността. Резултатите са категорични, че 73 % от разузнавателните служби, ангажирани с проекти по киберсигурност, оценяват потенциала на блокчейн като основополагащ и ключов за бъдещото развитие на информационната инфраструктура и резултатност в разузнавателните процеси и дейности.

Европейски съюз

- Европол интегрира блокчейн за проследяване на криминални трансакции;
- ENISA[4] разработва препоръки за използване на блокчейн в киберсигурността [8];
- Съвместни проекти между разузнавателни служби на държавите членки.

Френски изследователи от CNRS[5]отбелязват, че блокчейн платформите „позволяват по-голяма прозрачност и проследимост на чувствителни данни“ [7]. Тези резултати подкрепят тезата, че въвеждането на блокчейн технологиите ще повиши ефективността на разузнавателните операции по отношение на борбата с киберзаплахи и атаките.

Китай

Китайските научни публикации, като тези от Китайския институт за блокчейн, подчертават необходимостта от държавен контрол и стандартизация, като се обръща специално внимание на интегрирането на блокчейн в системите за национална сигурност. Според доклад от 2021 г. [6] над 80 % от държавните проекти с блокчейн в Китай са насочени към подобряване на сигурността и управляемостта на критични данни.

---

[1] ***Defense Advanced Research Projects Agency.*** Агенцията за перспективни изследователски проекти за отбраната е научноизследователска и развойна агенция към Министерството на отбраната на Съединените щати, която се занимава с развитието на новите технологии в американската армия [12].

[2] **National Security Agency.** Агенцията за национална сигурност е разузнавателна организация на САЩ. Тя е най-голямата, най-скъпо оборудваната и технологично най-напреднала разузнавателна агенция на планетата [18].

[3] **Central Intelligence Agency (CIA).** Централното разузнавателно управление (ЦРУ) е държавна американска разузнавателна агенция, събираща и обработваща информация за чужди правителства, организации, фирми и граждани [20].

[4] **European Union Agency for Cybersecurity** [16].

[5] **Centre national de la recherche scientifique.** Френският национален център за научни изследвания е най-голямата агенция за фундаментална наука в Европа [15].

Таблица 1. **Степен за внедряване на блокчейн по посочени критерий**

Критерий	***България***	***Франция***	***САЩ***	***Китай***
Сигурност	Използване на установени криптографски стандарти [4]; Нормативна рамка се разработва и все още не се прилага	Силно регулирана от закона за защита на данните; Акцентът е върху киберсигурността	Използване на модерни технологии за криптографска защита и множество нива на одит и мониторинг	Цялостна държавна стратегия с акцент на интегрирането на национални стандарти за информационна сигурност
Проследимост и отчетност	Стремеж към въвеждане на децентрализирани системи за гарантиране на проследимостта на данните	Изисква прозрачност в обработката на данни в рамките на националните регулаторни изисквания	Подчертаване на неизменяемостта на записите чрез разпределителната книга на блокчейн	Законодателство, което насърчава проследимост и контрол върху данните, включително чрез блокчейн решения [5]
Мащабируемост и скорост	Извършват се пилотни проекти; Предизвикателства с мащабируемостта и анализа на големи данни	Разработват се експериментални проекти за подобряване на скоростта и ефективността	Различни индустриални решения, но проблемът остава център на иновациите с висок обем данни	Вложени са значителни ресурси в оптимизация на протоколите за обработка на данни в реално време
Интероперативност	Трудности с интеграцията със съществуващите държавни системи; Постепенно приемане	Насърчаване на съгласуваност между институциите чрез стандартизация и общи протоколи	Акцентът е върху интегрирането с частния сектор и междуплатформената съвместимост	Поддържане на централизирана база данни с възможности за свързване с международни системи
Регулаторна съвместимост	В основата е поставен Законът за защита на личните данни	Силно регламентирано от държавни нормативни актове; Използване на Регламента за защита на личните данни като модел	Рамки, които интегрират критични инфраструктурни мерки и закони за национална сигурност	Разработени са специфични регулаторни документи за засилен контрол от страна на държавата

От сравнителният анализ става ясно, че всяка от разглежданите държави внедрява и използва блокчейн в разузнаването, за да изпълни конкретни поставени цели според политическа обстановка и приоритети:

- **България** се насочва към актуализирането на съществуващата нормативна рамка, като интеграцията на блокчейн става ключов елемент в подобряването на националната сигурност и управлението на данните.
- **Франция** и **Англия** поставят акцент върху съчетаването на иновациите със стандартните системи за сигурност, като прилагат хибридни решения. По този начин се улеснява обменът на информация между частния и публичния сектор [10].

▪ **Китай** интегрира блокчейн в дългосрочни стратегически инициативи, подкрепени от огромни държавни инвестиции, съпроводени с национална политика, насочена към централизирано управление на данните с оперативен контрол и мониторинг [10].

Според проучване на Rand Corporation [19] към 2030 г. над 60 % от разузнавателните агенции ще използват блокчейн за поне един основен процес.

Заключение

Интеграцията на блокчейн технологията в разузнаването представлява революционна възможност за повишаване на сигурността, прозрачността и ефективността на събирането и обработката на данни. Блоковата верига дава възможност за модернизиране на разузнавателната дейност, като подобрява сигурността и защитата на информацията, ефективното междуведомствено сътрудничество и по-добрата проследимост и отчетност на данните.

Успешното внедряване на блокчейн в разузнаването изисква редица анализи и процеси, които да актуализират правнонормативната рамка, да се направи плавно и внимателно планиране с поетапен подход. Задължително условие е да се направи адекватно и последващо обучение на служителите за промяна в работните процеси и среда.

Литература

1. **Закон** за управление и функциониране на системата за защита на националната сигурност. [онлайн]. *https://lex.bg/bg/laws/ldoc/2136641510.*
2. **Личева,** Т. Блокчейн и екосистема на сигурност. – В: *Сборник* с доклади от научната конференция „Актуални проблеми на сигурността“, 27 – 28.10.2022 г., с. 141 – 148. ISSN 2367-7473.
3. **Личева,** Т. Блокчейн сигурност на личните данни. – В: *Сборник* с доклади от научната конференция „Актуални проблеми на сигурността“, 27 – 28.10.2023 г., с. 127 – 137. ISSN 2367-7473.
4. **Радулов,** Н. Сигурност 4.0. София: НТС по машиностроене „Индустрия 4.0“, 2019. ISBN 987-619-7383-15-7.
5. 《中华人民共和国网络安全法》. (Закон за киберсигурността.) Народна република Китай, 2017.
6. **China** Blockchain Research Institute. Annual Blockchain Development Report. Beijing, 2021.
7. **CNRS.** Études sur la traçabilité des données sensibles à l'aide de la technologie Blockchain. – In: *CNRS* Research Bulletin, 2018.
8. **European** Union Agency for Cybersecurity (ENISA). Blockchain and Cyber security Guidelines. ENISA Publications, 2020.
9. **Zegart,** A. Spying Blind: The CIA, the FBI, and the Origins of 9/11. Princeton University Press, 2020.
10. *https://dtf.aadcf.nvu.bg/wp-content/uploads/2024/01/DTF-2023.pdf*
11. *https://en.wikipedia.org/wiki/Central_Intelligence_Agency*
12. *https://en.wikipedia.org/wiki/DARPA*
13. *https://en.wikipedia.org/wiki/In-Q-Tel*
14. *https://ieeeaccess.ieee.org/*
15. *https://www.cnrs.fr/fr*
16. *https://www.enisa.europa.eu/*
17. *https://www.ipa.government.bg/sites/default/files/strategichesko_prognozirane_analiz.pdf*
18. *https://www.nsa.gov/*
19. *https://www.rand.org/*
20. *https://en.wikipedia.org/wiki/Central_Intelligence_Agency*

КОНКУРЕНТНОТО РАЗУЗНАВАНЕ В СЪВРЕМЕННИ УСЛОВИЯ – ОСНОВА НА КОРПОРАТИВНАТА СИГУРНОСТ

д-р Костадин Язов
Висше училище по сигурност и икономика – Пловдив

COMPETITIVE INTELLIGENCE IN MODERN CONDITIONS – THE BASIS OF CORPORATE SECURITY

Kostadin Yazov, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Понятието „конкурентно разузнаване“ е известно още като бизнес разузнаване. Общността на професионалистите от конкурентното разузнаване (SCIP) под „конкурентно разузнаване“ разбират планирани действия на фирмите по систематично и етично събиране, анализ и управление на тази информация за външната среда, която може да повлияе при осъществяването на плановете на предприятието и неговата работа като цяло. Конкурентното разузнаване е дейност, която осигурява ръководството на фирмата с информация, необходима за изпреварващо вземане на решение. Това не е само придобиване на информация, но и нейното класифициране, анализ и прогноза за развитието на ситуацията и подготовка на препоръки към ръководството. Нуждата от информация за конкурентите като че ли автоматически поставя въпроса за корпоративната сигурност.*
Ключови думи: *бизнес разузнаване; търговско разузнаване; конкурентно разузнаване; информационно разузнаване; организация; нелоялна конкуренция*

Abstract: *The concept of competitive intelligence is also known as business intelligence. The Society of Competitive Intelligence Professionals (SCIP) defines competitive intelligence as planned actions of companies to systematically and ethically collect, analyze and manage information about the external environment that can affect the implementation of the company's plans and its work as a whole. Competitive intelligence is an activity that provides the company's management with the information necessary for anticipatory decision-making. This is not only the acquisition of information, but also its classification, analysis and forecasting of the development of the situation and the preparation of recommendations to the management. The need for information about competitors seems to automatically raise the issue of corporate security.*
Key words: *business intelligence; Commersial Intelligence; Competetive Intelligence; Information Warfare; organization; unfair competition*

Характеристика на конкурентното разузнаване

За живота в съвременния свят в условията на конкурентна борба на всички равнища първостепенно значение имат както разкриването на намеренията на конкурентите и изучаването на основните тенденции в бизнеса, така и анализът на възможните рискове. Тази дисциплина на Запад се нарича „Конкурентно разузнаване“. В съответната литература по този въпрос се срещат още и термините „делово разузнаване“, „бизнес разузнаване“, „икономическо разузнаване“ – термини като еквиваленти на конкурентно разузнаване (КР). За дейността на конкурентното разузнаване в качеството на субект се явява всяка недържавна организация – частна фирма, банка, акционерно дружество.

Всъщност в исторически план конкурентното разузнаване е възникнало още в дълбока древност, а първият известен автор по тази тема за всички аспекти на разуз-

наването е Сун Дзъ (Sun Tzu) – небезизвестният китайски военачалник и стратег, живял около 500 г. пр.Хр. Неговият знаменит труд „Изкуството на войната“ се изучава и до днес както от военни експерти и държавни ръководители, така и от мениджъри и специалисти в различни области на бизнеса. В него Сун Дзъ се фокусира върху важността на разузнаването и широката осведоменост от средата при планиране на военни действия.

Подходите и методите, използвани от разузнаването, се променят и разширяват през различните епохи, като отговарят на времето, в което се развиват. Още в далечните времена на Египет, Древна Гърция и Рим най-опитните търговци тайно придобивали информация, която да им помогне в преговори и сделки, като някои от тях паралелно предприемали и действия за злепоставяне на конкурентите по множество начини. Разузнаването преминава през вековете своето развитие, като в различните епохи водещи в процеса на разузнаване са различни държави според собственото им развитие, особено ако се фокусираме върху епохата на Великите географски открития, когато сериозно се развива битката за надмощие на страните над новооткритите територии.

В САЩ идеята за по-сериозно използване на дейности, свързани с маркетингови проучвания, анализ на конкуренцията, конкурентни сили се заражда около края на XIX в. и еволюира постепенно, за да стане задължителна част от оперативната дейност на компаниите и досега.

По време на Втората световна война се засилва икономическото разузнаване за врага, а след нейния край вече събраната информация повлиява в огромна степен при преразпределението на следвоенния глобален пазар. Развива се в държавите на азиатския континент, като най-сериозно се проявява по време на Суданата война между САЩ и СССР.

Днес повече от всякога се залага на бизнес разузнаването, на което се разчита не само от малки, но и от големи компании. То спомага за взимане на управленски решения на базата на получена и анализирана информация.

Трябва да се обърне внимание още и на необходимостта от спазване на съществуващите правни норми, което отличава конкурентното разузнаване от шпионажа [1: 37], където необходимите сведения могат да се получават или намират и извън законовия ред. Затова може да се даде и такова определение за „конкурентно разузнаване“: „Конкурентно разузнаване“ се нарича дейността на недържавните институции с цел получаване на сведения за реална или потенциална заплаха за тяхното съществуване и техните интереси при спазване на дадените правни норми“ [4: 48]. Конкурентното разузнаване е мощен инструмент в изследването на пазара и в съвременните условия е динамично развиваща се структура, възникнала при взаимодействието между икономика, юридическо право и специални разузнавателни средства. За разлика от промишления шпионаж конкурентното разузнаване се осъществява изключително на базата на съществуващите държавни закони и получава своите резултати благодарение на аналитичната обработка на огромно количество най-разнообразни информационни данни, получени от открити източници. Конкурентното разузнаване работи само с открити източници на информация. Терминът „разузнаване“ подчертава сходството на задачите и методите, използвани в дейността на държавните специални служби и деловите структури.

Терминът „корпоративно разузнаване“ се използва за разузнавателните структури на корпоративно ниво, особено що се отнася до ТНК, и се реализира посредством два начина – чрез собствено звено в структурата на корпорацията или чрез специализирана външна агенция [4: 79]. Икономическото разузнаване представлява допълнение към политическото и военното разузнаване, като по-голямата част от разузнавателните сведения са от открити източници.

Целите и задачите на конкурентното разузнаване в много отношения са близки до целите и задачите на класическото разузнаване, чиито анализи се използват при формирането и осъществяването на държавната политика и при планирането на военни операции, при което само мащабите на решаваните задачи са съвършено различни. Главната цел на конкурентното разузнаване е системното наблюдение и събиране на информация за конкуренцията, анализ на получените данни и вземане въз основа на тях правилни управленски решения. Развитието на пазарните отношения води до появата на икономически структури с различни форми на собственост. Между тях се води остра конкурентна борба за пазарни територии, за кадри, технологии, инвестиции, като се допуска при това тя да се води и с непозволени средства. Затова в съвременните условия на живот проблемите с осигуряването на безопасност в предприемаческата дейност са особено актуални. Основната област, в която се развива конкурентното разузнаване, е пазарът.

Създаването на конкурентно разузнаване [2: 24] позволява да се предвиждат промените на пазара, да се прогнозират действията на конкурентите, да се провежда мониторинг при появата на нови технологии и политически рискове. Конкурентното разузнаване подобно на мощен радар прихваща новите прояви в бизнеса, новопоявящите се възможности и предупреждава за приближаващи опасности. В крайна сметка с разширяването на мрежата на интернет и появата на компютърните бази данни информацията се превръща във важна и напълно достъпна стока и заради нейната поява няма смисъл да се обременява корпоративната структура с още едно подразделение. Задачата на конкурентното разузнаване се състои главно в помощта, която трябва да се окаже на ръководството на дадена компания да извлече от големия информационен поток само необходимите за вземане на правилни решения данни. Както казва авторът на книгата „Конкурентно разузнаване“, Л. Каханер: „Ние живеем не във века на информацията, а във века на разузнаването“.

В основата на системата на конкурентното разузнаване стоят т.нар. „етапи“ в неговата дейност, чрез които суровата информация се превръща в систематизирани данни.

✓ Планиране – Това е етапът на вземане на решение за получаване на достоверни аналитични данни за дейността на конкурентите. Определят се какви действия трябва да се предприемат, за да се реши дадената задача. Един етап може да бъде начало и на следващ, тъй като лицето, получаващо първичната информация, може да реши да постави пред конкурентното разузнаване допълнителни задачи, водещи до нов етап в разследването.

✓ Събиране на информация – През този етап се търси и събира сурова информация, въз основа на която ще се подготвят разузнавателните сведения. По-голямата част от информацията ще се получи от достъпни за всеки, знаещ къде да търси, източници. Към тях се отнасят периодичните издания, ежегодните отчети на фирмите, книги, сборници, радио- и телепредавания, изказвания, наличната база данни в интернет пространството и др. Изобретателните „събирачи“ на информация обикновено намират по-голямата част от нея, без да нарушават общоприетите в обществото норми. Този етап включва предварителната обработка на информацията (оценката, квалификацията, представянето в електронен вид), което позволява при необходимост тя да се предава, съхранява и обработва чрез използване на цифрова технология – всичко, което е съвършено необходимо за следващия етап.

✓ Анализиране на информацията – Обикновено това е най-трудният етап в целия цикъл на работа на конкурентното разузнаване. Този етап изисква истинско майсторство от анализиращите, които трябва да преценят събраната информация, да я срав-

нят с вече наличната и да подготвят различни възможни сценарии за развитие на ситуацията. Дори когато анализът се базира на логически изводи и проверени достоверни данни, анализаторът трябва понякога да предугажда ситуацията и да представя обосновани предположения за евентуалното развитие по един или друг начин на събитията.

✓ Представяне на анализираните данни – Това е последният в целия процес на конкурентното разузнаване етап (той може да се превърне в първи в ново, бъдещо разследване). Това е етап на предаване на събраните с много труд разузнавателни сведения към лицата, за които са предназначени. Анализаторите могат да предлагат варианти на действие, основани на получените резултати. Анализаторите трябва ясно и точно да формулират своите предложения и да са подготвени да ги защитят пред ръководството на компанията. Тези резултати трябва да бъдат достъпни и за другите специалисти от същата компания.

Не трябва да се пренебрегва фактът, че сведенията, които предоставя на дадената компания конкурентното разузнаване, трябва да са актуални към момента на тяхното използване.

Успешно внедрените и работещи програми по конкурентно разузнаване не само носят знания за средата, в която функционира бизнесът, но и създават условия за предупреждения относно съществуващи или потенциални възможности и заплахи.

Идентифицирането на нуждата от разузнавателна информация и последващото ѝ събиране и анализ са ключов етап от цялостния цикъл на конкурентно разузнаване в бизнеса.

Цикъл на развитие на конкурентното разузнаване

Основно изискване, стоящо твърде често пред службите за конкурентното разузнаване на отделните компании или детективски агенции, занимаващи се с проверка на даден партньор или конкурент, е събирането на всякаква възможна информация за съответната конкуренция. При това не се и конкретизира крайната цел на операцията. Сътрудниците от службата за конкурентното разузнаване или детективите извършват огромна по обем и вложен труд работа, в резултат на която се събират много като количество разнообразни факти, данни, слухове, пряко или косвено касаещи изследвания въпрос. Но твърде често цялата тази дейност се оказва слабоефективна, тъй като отделни необработени факти, та дори и най-интересните, не представляват кой знае каква ценност при взимане на съответните решения. За да се избегне такава ситуация, процесът на конкурентното разузнаване трябва да протича по определени правила, които се определят като цикъл в развитието на конкурентното разузнаване.

Конкурентното разузнаване дава най-добри резултати, когато е организирано като непрекъснат процес.

✓ На първо място, структурата на цикъла на развитие на конкурентното разузнаване сама по себе си вече предполага наличието на процес. При организирането на широкомащабна система на конкурентното разузнаване в собствената компания нейният ръководител/собственик трябва винаги да се стреми към разширяване на сферите на дейности извън самата компания и към привличане за сътрудничество на колкото е възможно повече хора.

✓ На второ място, обезпечаването на достъп до данните на конкурентното разузнаване само за мениджърите от най-високо ниво може понякога да „лиши“ компанията от други сътрудници, кото биха искали да имат тези данни и да ги използват в своята работа. Може да се създаде високоефективна система на управление на компанията, тя да има висококвалифицирани специалисти, да притежава висок научно-технически потенциал, да има широкоразкроена работна мрежа, а в същото време да

се окаже, че всичко това не е толкова важно, ако собственикът/ръководителят на фирмата или компанията е неспособен да прецени и предвиди външните заплахи и рисковете, които могат да поставят компанията или фирмата в един момент в сложна ситуация. И не е така важно къде ще бъде разположено като работно звено конкурентното разузнаване. Важно е как е организирана координацията на неговата работа и как циркулират информационните потоци вътре в компанията или фирмата. За максимална ефективност на работата подразделението на конкурентното разузнаване трябва да има достатъчно висок статут в самата компания, за да го уважават всички и да виждат в негово лице защитник на своите и на компанията интереси. Но в същото време подразделението на конкурентното разузнаване трябва да бъде и достъпно за всеки работещ във фирмата или компанията, а не само да изпълнява задачи в интерес на един или друг отдел. Анализираната информация, подготвена от конкурентното разузнаване, трябва да бъде недостъпна за всички външни лица, но и достъпна за всеки от сътрудниците на самата компания.

Технология и принципи на разузнаването

Разузнаването – това е технология за събиране, обработване, анализ на информация и синтез на знания, необходими за реализацията на конкретни цели.

Конкурентното разузнаване [4: 114] осигурява събиране и обработка на информация, за бизнеса и само за бизнеса, в интерес на бизнеса, използвайки легални и етични методи, при които явленията и тенденциите се разглеждат през призмата на конкуренцията и конкурентната борба.

✓ Конкурентното разузнаване е: информация, анализирана до ниво, осигуряващо вземането на необходимото адекватно решение.

✓ Инструмент за своевременна подготовка на управлението на бизнеса за потенциални заплахи и нови възможности.

✓ Средство за разумни оценки. Конкурентното разузнаване предоставя приблизителни и много добри обзори на състоянието на пазара и конкуренцията.

✓ Възможност за множество приложни оценки.

✓ Път за подобряване на пазарните позиции на компанията.

✓ Жизнен път на компанията. При правилно организиране и използване конкурентното разузнаване се превръща в жизненонеобходимо за всеки сътрудник от компанията. Конкурентното разузнаване е процес, благодарение на който критично важната информация става достъпна за всеки нуждаещ се от нея.

✓ Способ за наблюдаване на компанията отстрани. Компаниите, които ефективно развиват и прилагат конкурентното разузнаване, получават възможност да видят себе си отстрани.

✓ Прогноза – краткосрочна и дългосрочна. Едни и същи данни могат да бъдат използвани за разработване и коригиране на дългосрочния стратегически план за развитие или за определяне на пазарните позиции на компанията.

Процесът на глобализация на света, разпространението на интернет и достъпността на неограничено количество бази данни в откритите източници на информация влияят положително на конкурентното разузнаване в световен мащаб. Мениджърите и управителите на фирми много често прибягват до услугите на конкурентното разузнаване. Освен на разузнаването на чужди тайни, трябва да се обърне внимание и на запазването на собствените тайни, което от своя страна е поверено на отделите на контраразузнаване. Агентите от конкурентното разузнаване водят безмилостна война с нелоялната конкуренция и промишления шпионаж.

Следването на етическите норми на поведение при провеждането на конкурентно разузнаване е не само правилно от морална гледна точка, но и икономически изгодно. Етичното поведение спасява фирмата от различни разходи за водене на съдебни дела и свързани с тях загуби. Друга причина е, че такова поведение гарантира спокоен, безпроблемен живот. Третата причина е доверието към компанията и общественото мнение.

Етическият кодекс – ако той съществува – включва норми на поведение и на сътрудниците на конкурентното разузнаване. В течение на дълго време привържениците на такова поведение твърдят, че нарушаването на нормите за морал и снижаването на етическите критерии за поведение на обществото водят до големи загуби при осигуряване на неговата безопасност. В същото време обаче, макар и толкова млада дисциплина, за конкурентното разузнаване важат старите истини. Една от тях гласи: „85 % от информацията, която ни е необходима, се намира за обществено ползване. Другите 15 % може и никога да не ни потрябва“.

Заключение

В крайна сметка при спазването на законите, нормативните уредби, етическите и моралните норми конкурентното разузнаване се оказва незаменим сътрудник и мощно оръжие за управителите на големите компании и малките фирми в цял свят.

Разузнавателните термини се отнасят до използването на систематични методи на събиране, анализ и разпространение на информация, поддържаща процеса на вземане на решения. Може да се направи изводът, че конкурентното разузнаване е с най-широк обхват на разузнавателни дейности, които обхващат цялата външна работна среда на компанията, и насочване на всички нива на вземане на решения, т.е. стратегически, тактически и оперативни.

Конкурентното разузнаване играе важна роля в съвременния свят и служи да открие и формулира ранно предупреждение за заплахи и проблеми в бизнеса. Неговата роля е да подпомогне формулирането и развитието на бизнес процесите в организацията, които се отнасят до намаляване на разходите, до по-ефективно управление на ценовите предприемачески и маркетингови стратегии на компанията, както и да подпомогне създаването на нови продукти.

В заключение може да се направи извод, че през последното десетилетие конкурентното разузнаване има пряко отношение към принципите на съвременното предприемаческо управление на организациите и корпорациите, както и към тяхното развитие.

Литература

1. **Бояджиев,** Т. Шпионажът като занаят. София: Захарий Стоянов, 2002. ISBN 954-739-28-67.
2. **Баяндин,** Н. И. Технология на безопасността на бизнеса: Въведение към проблема на конкурентното разузнаване. Учебно-практическо пособие. Москва: Юристь, 2002.
3. **Доронин,** А. Аналитична обработка на материали от открит достъп. БДИ, 1999.
4. **Начев,** Й. Конкурентно разузнаване – частна разузнавателна дейност. София: Сиела-Софт енд пъблишинг, 2007. ISBN 978-954-28-0025-5.
5. **Петров,** А. Активна корпоративна сигурност. София: Свят и наука, 2007.
6. **Портер,** М. Конкурентная стратегия: Методика анализа отраслей и конкурентов. Москва: Альпина Бизнес Букс, 2005. ISBN 978-5-9614-0143-0.
7. **How** Competitors Learn Your Company's Secrets. – In: *Washington* Researchers, 1997, p. 14.
8. **Weiss,** Arthur. A brief guide to competitive intelligence: How to gather and use information on competitors. Aware, 2002. [online]. *https://www.researchgate.net/publication/247759528_A_brief_guide_to_competitive_intelligence_How_to_gather_and_use_information_on_competitors,*

СЪВРЕМЕННОТО РАЗУЗНАВАНЕ
И КОНТРАРАЗУЗНАВАНЕ
И СЛУЖБИТЕ ЗА СИГУРНОСТ
И ОБЩЕСТВЕН РЕД –
ИСТОРИЯ, СЪСТОЯНИЕ,
ВИЗИЯ ЗА РАЗВИТИЕ

ДЪЛБОКАТА ДЪРЖАВА, РЕФОРМАТА НА ПОЛИТИЧЕСКАТА СИСТЕМА И СЛУЖБИТЕ ЗА СИГУРНОСТ В РЕПУБЛИКА БЪЛГАРИЯ

проф. д.п.н. Георги Л. Манолов
Висше училище по сигурност и икономика – Пловдив

THE DEEP STATE, THE REFORM OF THE POLITICAL SYSTEM AND THE SECURITY SERVICES IN THE REPUBLIC OF BULGARIA

Prof. Georgi L. Manolov, DPS
Higher School of Security and Economics – Plovdiv

Резюме: *В настоящия доклад систематично са разгледани същността и характеристиката на т.нар. „дълбока държава“ и нейното функциониране в Република България. Посочени са и фундаменталните лостове за реформиране на политическата система (конституционна реформа, нов избирателен кодекс, съдебна реформа, административна реформа и електронно правителство и др.) като ключов механизъм за демонтиране на дълбоката държава. В този контекст са изведени и някои съществени мерки за изменение и демократизиране на службите за сигурност в страната.*

Ключови думи: *държава; дълбока държава; политическа система; служби за сигурност*

Abstract: *This report systematically examines the nature and characteristics of the so-called „deep state“ and its functioning in the Republic of Bulgaria. It also identifies the fundamental levers for reforming the political system (constitutional reform, new electoral code, judicial reform, administrative reform and e-government, etc.) as a key mechanism for dismantling the deep state. In this context, some essential measures for changing and democratizing the security services in the country are also outlined.*

Key words: *state; deep state; political system; security services*

Напоследък проблемите, свързани с т.нар. „дълбока държава“, непрекъснато намират място в широкото публично и медийно пространство. Това с особена сила е валидно след последните американски избори за президент (2024 г.), след които новият владетел на Белия дом обяви тотална война на тази държава по всички възможни направления – политически, икономически, търговски, културни, международни и др. И ако приемем тезата, че „дълбоката държава“ е пуснала дълбоки корени в целия демократичен свят (и особено в Европа), то логично възниква въпросът какви са нейните измерения и в България, тъй като сме част от двете ключови организации на нашия континент – Европейския съюз (ЕС) и Северноатлантическия пакт (НАТО). В този смисъл първо ще се опитаме да дадем отговор на въпроса за същността и характеристиката на „дълбоката държава“ (ДД) в България, след това на необходимостта от реформиране на политическата система като фундаментален лост за преодоляване на влиянието на тази държава и най-накрая ще изложим виждането си за ролята и мястото на службите за сигурност в контекста на радикалната политическа реформа в страната.

Същност и характеристика на дълбоката държава

Понятието „дълбока държава“ няма еднозначно наименование и предназначение и обикновено се идентифицира с такава власт, която няма почти нищо общо с

официалната легитимна власт, независимо че функционира след провеждането на законни конституционни избори. С този феномен с продължение на векове успешно се манипулират редица народи и държавни институции, което е друго важно измерение на неговата същност, поради което притежава множество разнообразни наименования, като: „двойна власт“, „паралелна власт“, „вторична власт“, „анонимна власт“, „скрита власт“, „правителство в сянка“, „държава в държавата“, „дълбока власт“, „нелегитимна власт“, „сенчеста власт“ и т.н., и т.н.

В този контекст съществуват и десетки различни дефиниции на понятието „дълбока държава“, част от които ще изложим в настоящия текст.

Още в началото на XX в. известният американски президент **Теодор Рузвелт** (1901 – 1908 г.) недвусмислено дефинира „дълбоката държава“ по следния начин: „Зад привидното правителство седи невидимо правителство, навярно и непризнаващо никаква отговорност към хората. Да се унищожи това невидимо правителство, този мръсен и нечестен съюз между корумпирания бизнес и корумпираните политици е първата задача на държавническата мисия на деня“ [4: 158].

Според един от най-признатите специалисти, атакуващи характеристиките на тази държава, американеца **Майк Лофгрен,** дълбоката държава е „*масивна структура, състояща се от мрежа от изключително арогантни, високоинтелигентни и много мощни вградени висши държавни служители, както и от елитни институции и техните лидери, които оправдават поведението си чрез процес на разсъждение, който свързва цели и средства, единство на противоположностите, термин, напълно съвместим с марксистката диалектика, независимо дали практикуващите го осъзнават с това име или не“.* И още, това е „*хибридна асоциация от елементи на управление и части от финансова и индустриална организация, които ефективно могат да управляват Съединените щати без съгласието на управляващите, изразено чрез формалния политически процес“*[6; 4: 56].

Съдържателна дефиниция предлага и шведският **проф. Ола Тънандер,** за която дълбоката държава е „*повече или по-малко скрита „йерархия на сигурността“, или „държава на сигурност“, която не само действа паралелно на официалното правителство, но и упражнява контрол над „редовната държавна йерархия“* [4: 57].

В единствената засега монография по разглеждания проблем българският учен **проф. Йордан Начев** извежда едно много стойностно и обосновано определение, което гласи, че „дълбоката държава е корпоратизирана, милитаризирана, бюрократично стабилна и ефикасно функционираща група с неизбран от хората състав, който в действителност ръководи страната. Дълбоката държава действа като правителство в сянка и представлява скритото лице на организация, която не зачита свободата на своите граждани“ [4: 58][1].

Без да игнорираме различните дефиниции, които изложихме по-горе, можем да детерминираме **„дълбоката държава“ като тесен олигархичен кръг хора (политически, икономически, бизнес и друг елит) и свързаните с него обслужващи слоеве, които зад маската на законни избори и почти винаги, без да участват пряко във властта, реално упражняват политическата власт (законодателната, изпълнителната, съдебната) в държавата на всички йерархични равнища.** Това е **паралелна политическа власт,** чиито представители в действителност взимат важните управленски решения в името на добре прикрити лични, партийни, корпоративни интереси; това е **анонимна политическа власт,** чиито представители са скрити под сянката на легитимните политически институции, успешно манипулирайки обществено-

[1] Тази определеност на „дълбоката държава“ е разгледана на базата на значителна част от най-стойностните дефиниции на това понятие в литературата, което придава допълнителна положителна стойност при интерпретацията на настоящата проблематика (Вж. още [4: 53 – 68]).

политическия живот в своя лична, партийна или друга изгода; и най-после, това е рафинирано **делегитимиране на властта,** при което действащите централни институции – парламентът, правителството, съдът, прокуратурата и др., по същество „абдикират“ от своите законови правомощия под прикритието на конституционните си функции в услуга на антинародни колективни групови интереси.

Задължително трябва да се отбележи, че в центъра на дълбоката държава като неин основен субект се позиционира политическата власт на държавата и нейните висши институции, чрез чието „завладяване“ се реализират тъмните недемократични, корупционни и корпоративни интереси на „дълбоката държава“ чрез съответните нелегитимни и легитимни представители във властта.

В зависимост от изведеното определение изрично се налага да подчертаем, че в устоите на политическата власт (и институции) трайно са се загнездили цяла кохорта взаимнозависими и преплетени скрити (и открити) слоеве и персони на ДД, които изключително рационално задвижват нейния огромен механизъм. Той се състои от цяла редица важни институции, специфични слоеве и агенти за влияние, чрез които по перфектен начин осигуряват неговата „качествена“ работа в интерес на адептите на „дълбоката държава“. Или, иде реч за безупречна държавно-частна трансмисия, която посредством своите основни слоеве и агенти за влияние изцяло постига пъклените си планове и намерения за изпомпване на националното богатство със законни (обществени поръчки) и незаконни (нелегитимни начини) средства *(вж. Фигура № 1).*

От предложената фигура се вижда, че в нея основно могат да се открояят три опосредстващи зависимости при функционирането на „дълбоката държава“: 1) това е **т.нар. „вертикално равнище (и връзки)“,** което приоритетно се разгръща около структурите на висшата държавна власт (парламента, правителството, съда) като стройна йерархична структура, която тотално се използва и контролира от проводниците и агентите за влияние от горе до долу, за да се придобиват огромни финансово-парични изгоди в полза на субектите на ДД; 2) следващата зависимост е на **т.нар. „хоризонтално равнище (и връзки)“,** където различни бизнес субекти, корпорации, фирми, партии, личности и др. като лиани са увити около структурите на съответната власт – централната, междинната (областната) и местната, държейки в ръцете си и разпределяйки ключови властови, политически и икономически ресурси; 3) и последната зависимост е на **т.нар. „директно или пряко равнище (и връзки)“,** при което взаимните връзки между субектите на ДД са непосредствени, конкретни и персонални, целящи разпределяне и преразпределяне на обществени блага и услуги с официалното „съдействие“ на самата държава.

Не е трудно да се забележи, че общото и за трите равнища на взаимодействие и функциониране на дълбоката държава е това, че **агентите и слоевете на тази държава изобщо не могат да функционират (и съществуват) без политическата власт и респективно да оказват огромно негативно влияние върху цялостното развитие на държавата и обществото,** доколкото реализират не държавни, а частни или корпоративни интереси на съответните социални слоеве.

Въз основа на формулираната дефинитивна същност на дълбоката държава в България нека посочим и нейните основни характерни черти, които ярко прозират в цялостния социалнополитически живот на страната.

Първо. Почти формално и безсъдържателно функциониране на водещите институции и системи на държавата – парламента, правителството, съдилищата, прокуратурата и др.

Фигура № 1. ***Основни слоеве, проводници и агенти за влияние на дълбоката държава***

Второ. Обезличаване и **„заместване“ на ролята и функциите на държавните институции със скрити нелегитимни решения,** прокарвани от олигархични персони и лобисти, които са „облечени“ в държавни норми (закони, постановления, решения, наредби, правилници и др.).

Трето. Дълбоко ешелониране в „тила“ на държавните институции на скрити (и открити) представители на олигархично-лобистки групи за влияние на всички равнища на властта – по хоризонтала и вертикала (законодателна, изпълнителна, съдебна).

Четвърто. Формиране на послушен, покорен и раболепен „политически елит“, който изцяло загърбва националните интереси, защото **безпрекословно служи и изпълнява повелите на босовете на дълбоката държава,** които здраво са стиснали този елит в „менгемето“ на всевъзможни компромати, тайни записи, нелицеприятни далавери и какво ли не още.

Пето. Тотално **влияние при взимането на политическите решения в държавата от страна на плутократични и олигархични кръгове,** скрити зад маската на обществените интереси.

Шесто. Монополно участие и **печелене на всички крупни държавни поръчки** (за милиони) и средства по линия на Европейския съюз само и единствено **от приближени фирми на мастити български олигарси** от плутократично, наследствено и номенклатурно потекло. Тоест тотално обсебване на икономиката.

Седмо. Назначаване на **лично предани персони и лица на ключовите висши длъжности във всички служби за сигурност (МВР, ДАНС, ДАР и др.),** които са протежета на мастити представители на дълбоката държава – политици, бизнесмени, олигарси, плутократи и др.

Осмо. Дълбоко проникване в структурите на държавната власт на знайни и незнайни персони на „сенчестия бизнес“, които перманентно „изпиват“ кръвчицата на изпосталялата (и сирота) българска икономика, безпощадно игнорирайки всякакъв обществен интерес в името на лични, партийни и корпоративни интереси.

Девето. Зловредна и **повсеместна корупция** (и корупционни схеми) **във всички социални области** – политическата, икономическата, духовната, културната и т.н., която дълбоко разяжда и обезличава имунната система на държавата, и преди всичко работата на нейните контролни органи и реализацията на техните функции.

Десето. Груба намеса при организацията на различните видове избори (парламентарните, президентските, местните) чрез **безскрупулна „търговия с гласове“, контролирания и купен вот,** както и мащабни манипулации и заплахи на електората по време на изборния процес.

Единадесето. Официално и неофициално **купуване на голяма част от медиите,** и особено на националните, посредством крупни суми за реклами, спонсорства, платени материали и др. с помощта на скрити собственици, бизнесмени и всякакви други подобни изпълнители (и поръчители).

Казано обобщено и по същество, със своите агенти, структури, форми, методи и начини на действие **дълбоката държава у нас неофициално (но реално) практически делегитимира законните държавни институции (парламента, правителството, съда и др.) и прокарва своите политически и икономически интереси чрез скрито и открито манипулативно въздействие посредством институциите, медиите, социалните мрежи и др.** Нещо повече, когато говорим за **България,** следва изрично да поясним, че **нашата дълбока държава е от плутократичен тип, т.е. нейните ключови представители са забогатели преди всичко от участие във властта (а не от почтен и нормален бизнес), от връзките си с разни олигархични структури, от прилагането на едни или други нелегитимни финансово-икономически**

схеми и т.н. С други думи тази дълбока държава с пълно основание може да се нарече **„дълбокоплутократична държава“** поради безспорния социален факт, че нейните ключови играчи притежават несметни богатства, натрупани от незаконни, „полузаконни“ и законни дейности благодарение на използването на властта в продължение на целия преход от тоталитарно към демократично общество.

Демонтиране на „дълбоката държава“ чрез реформиране на политическата система

Едва ли подлежи на съмнение обстоятелството, че когато говорим за премахване на „дълбоката държава“, ние винаги имаме предвид използването на конкретни и отделни законови форми (и начини) за изменение в отделни части и елементи на тази държава. Но въпросът тук според нас е много по-сложен, тъй като ДД е проникнала и буквално пронизва всички звена на българската политическа система като гигантски мафиотски октопод, който е обхванал (и обгърнал) с пипалата си абсолютно всички звена на тази система (политическата). Това на свой ред изисква прилагане на един цялостен комплексен подход, който да засегне дълбокото реформиране на ключовите елементи на политическата система, с които да се разбият, отстранят и демонтират структурите и елементите на „дълбоката държава“.

Когато у нас се говори за промени в политическата система, най-често се визират отделните ѝ части, което, макар и правилно, не е достатъчно, защото големият политически въпрос е съвсем друг: как да се реформират цялостно и резултатно всички елементи на българската политическа система, щото това да доведе до едно ново нейно качествено функционално състояние. Тоест необходима е **нова концептуална философия за реформиране на политическата система,** която да намери (и приложи) по-съдържателни подходи и механизми, особено за модернизиране на властовите институции в България. Тази философия трябва да се осъществява чрез предварително разчетени етапи в хода на политическия процес, като нейната реализация основно се разгръща по линия на представителната (непряката) и непредставителната (пряката) демокрация посредством следните по-съществени политико-правни мерки:

I. Представителна (непряка) демокрация

По-нататъшното бъдещо усъвършенстване на представителната демокрация у нас следва да обхване чрез реформиране всички съдържателни елементи на политическата система, а именно:

1) Конституционна реформа – извършване на дълбоки промени в сегашната конституция, при които (без да се изменя нейната демократична същност) да се изменят редица нейни клаузи, както следва: **намаляване на броя на депутатите на 160 души** и обмисляне на въпроса за формиране на втора камара на парламента (от около 40 души), за да се повиши качеството на парламентарната дейност; **приемане на закон за работата на Народното събрание** вместо досегашните правилници; въвеждане на **нови форми на контрол върху депутатите, включително и чрез отстраняването им от парламента** за несвършена работа по искане и с подкрепата на избирателите (най-малко на 2/3 от тях); **увеличаване на правомощията на президента** – предоставяне на правото му на законодателна инициатива и промяна в гласуването на президентското отлагателно вето от парламента (да става с 2/3 от депутатските гласове); **намаляване на мандатите на шефовете на съдебната власт** (на председателите на ВКС и ВАС и на главния прокурор) от 7 на 5 години; утвърждаване на нормата за **избиране от електората на съдиите и прокурорите** в средните звена на съдебната система (окръжните съдилища); **избиране на областните управители** по време на парламентарни или местни избори; **въвеждане на индивидуалната конституционна**

жалба до Конституционния съд като основно гражданско право; детайлно **прецизиране на правата на Великото народно събрание (ВНС) и Обикновеното народно събрание (ОНС),** като на ВНС се делегират правомощия само за приемане на нова конституция, докато на ОНС – всички останали права за промени, поправки, допълнения и изменения на основния закон.

Всичко, казано дотук, не би струвало и пукната пара, ако не се извърши в най-скоро време това народополезно дело – **радикалната промяна на българската конституция,** при това не откъм формата на управление на държавата, а преди всичко откъм отстраняване на онези нейни дефекти, които двадесетгодишната промяна неведнъж потвърди.[2] Защото без решителни изменения и допълнения на Конституцията нито синхронът между властите, нито откъснатостта на съдебната власт, нито всеядната политическа корупция, нито олигархичните елити във властта, нито всички, ама буквално всички политико-правни проблеми на българското общество биха получили някакво цивилизовано разрешение (вкл. и работата по демонтирането на ДД).

2) Нов избирателен кодекс

Политическата практика показа, че сегашният модел на пропорционална избирателна система у нас се оказва по-скоро „политическа спирачка“, отколкото рационален ускорител на развитието на демократичния политически процес. В този смисъл извършването на адекватна за нашите условия избирателна реформа е отдавна назряла потребност, която би трябвало да включва най-малко два възлови компонента: **промяна на избирателното законодателство** и на тази база – **смяна на пропорционалния избирателен модел** с друг, по-усъвършенстван и по-ефективен (даже и нов), с цел решително подобряване на качествения депутатски състав на Народното събрание. Акцентът при тази смяна следва да се съсредоточи върху три възможни варианта: **връщане към смесената избирателна система,** но ако се направят коренни подобрения, за да се отстрани „механичността“ на мажоритарния елемент в нея (както стана при вота за Великото народно събрание през 1990 г.); **приложение на обновена пропорционална система, основана на принципа на „панаширането“,** но чрез свободните партийни листи, където гласоподавателят съставя нова избирателна листа (от всички предложени), вписвайки в нея кандидати по своя собствена преценка; или използване на трети, смесен вариант от първите два; необходимо е да се приеме и нова, **по-висока избирателна бариера от порядъка на 5 %,** с което реално ще се ограничи достъпът на различни „партии лилипути“ до парламента, правителството и до финансовите ресурси, отпускани за тях (според законодателството).

Тук е мястото да вмъкнем и още едно рационално предложение – **приемане на закон за защита на правата на избирателите** (по американския опит), с който решително ще се ограничат проявите на манипулиране, изопачаване и фалшифициране на изборните резултати.

3) Съдебна реформа

Без никакво колебание ще изтъкнем, че реформата в съдебната власт е толкова закъсняла, че час по-скоро са необходими следните комплексни мерки: първо, приемане на **нов закон за съдебната власт,** в който ще се направят радикални организационни и кадрови промени (съобразно с необходимите изменения на сроковете и т. н.), ще се децентрализира прокуратурата (нещо, което не произтича от Конституцията), ще се въведе институцията на независимия прокурор, избиран от парламента и действащ по конкретни поводи за разследване на тежки престъпления и корупция във властта (както е по американския модел), и пр.; второ, **извършване на качествени**

[2] Последните изменения на българската Конституция от 2023 г. се оказаха твърде палиативни и непригодни и неслучайно по-голямата част от тях бяха отменени от Конституционния съд.

промени в атестирането, кадровото развитие и налагането на дисциплинарни наказания на магистратите, за да се подобри и модернизира работата на съдиите, прокурорите и следователите; и трето, изключително неотложни са **структурните промени в съдебната власт**, при които прокуратурата да премине в системата на изпълнителната власт (съответно МВР) с цел значително подобряване на синхрона между отделните видове власт и пр., и пр.

Ролята и значимостта на съдебната система у нас многократно ще порасне, ако българският законодател **промени Наказателния кодекс в частта му за налагане на сурови наказания на субекти и обекти на „търговията с гласове".** Тези наказания следва да са изключително тежки (като глоби и лишаване от свобода), за да стане най-после ясно на всички граждани в страната, че изборите не са търговска сделка, а велик демократичен акт.

Дори и само малка част от тези реформи в съдебната система да се извършат, не може да има никакво съмнение, че най-после ще се постави началото на ограничаването и поетапното ликвидиране на толкова тромавите и неефективни действия на съдебната власт, а оттук – и на резултатната борба с дълбоката държава и организираната престъпност. Това обаче не би могло да стане, ако в евентуален нов закон за съдебната власт не се **предвидят много по-адекватни и справедливи наказания за съдии, прокурори и следователи,** защото със сегашните „бележки" и „порицания", плюс супертромавия механизъм на тяхното налагане, нищо съществено няма да се промени.

4) Изпълнителна власт и електронно правителство

Провеждането на реформите в тази съществена сфера на държавната власт трябва да се извърши в четири ключови насоки: 1) **намаляване на броя на министерствата** в правителството чрез тяхното фиксиране в Конституцията (както е било в Търновската конституция); 2) въвеждане на директен граждански вот за премиер, или **всенароден избор на министър-председател,** което ще му делегира още по-големи морални отговорности и авторитет; 3) **провеждане на административна реформа,** която да реши два основни проблема – усъвършенстване на нормативната база и драстично намаляване на бюрократичната държавна администрация на т.нар. „агенции флуиди" и т.н.; и 4) **децентрализация на управлението на държавата** като основно средство за преодоляване на бюрократизма, с което да се постигнат няколко цели – обособяване на реални самоуправляващи се административно-териториални единици (области, общини, кметства), пряк контакт с хората и обратна връзка за решените проблеми, регулиране на структурите и броя на общините (и общинските служители) според потребностите и т.н., и т.н.; 5) **въвеждане на електронно правителство** като изключително ефективна мярка за борба с корупцията, беззаконието и агентите на ДД.

5) Антикорупционна политика (и законодателство)

Реализацията на предложените реформаторски мерки не би имала пълноценен успех без изготвянето на специална антикорупционна политика, която да се разгръща във висшите етажи на властта (т.е. от върха на управленската пирамида до нейната основа). Тази политика не бива да е конюнктурен палиативен акт, а да стъпва върху **държавна антикорупционна стратегия,** която да обхваща трите вида власт – законодателната, изпълнителната и съдебната, структурите на гражданското общество – неправителствените организации, фондациите, сдруженията, и всички граждани на държавата.

В центъра на тази стратегия трябва да бъдат приемането на закон за борба с корупцията и периодичното провеждане на **операция „Чисти ръце"** по аналогия с

италианския опит, чиято основна цел е парламентарното прочистване на целия държавен и общински апарат и администрация от корумпирани политици и служители, и т.н., и т.н.

6) Децентрализация на държавните дейности

При децентрализацията се изхожда от моментното състояние на държавата и от потребността от реформиране на нейните институции. Чрез нея (децентрализацията) следва да се предоставят все повече и повече функции, права и отговорности на местните органи на властта и самоуправлението, за да се решават още по-качествено и ефективно проблемите на хората. Това трябва да стане чрез решителна **промяна на действащите закони за местно самоуправление и местна власт** чрез делегиране на повече правомощия на кметовете и общинските съвети и други мерки.

Коренното реформиране на изпълнителната власт и държавната администрация в България може да се превърне в много ефикасен начин за борба с корупцията и организираната престъпност, ако към горните мерки се добави и **приемането на три нови закона – за борба с корупцията, за конфискация на имуществото на незаконно забогателите (преди и по време на прехода) и приемане на етичен кодекс на българските политици**. Такъв тип мерки, разбира се, е невъзможно да се осъществят без участието на другите власти, и особено на съдебните институции, но когато от политическите субекти е декларирана твърда политическа воля за пречупване на гръбнака на тези уродливи явления (корупция, престъпност и др.), властта наистина е в състояние сама да се справи с тях.

7) Промяна в дейността на политическите партии – без провеждане на коренни преобразувания в статута на политическите партии са невъзможни каквито и да са качествени реформи в институциите в държавата. Тези преобразувания трябва да се концентрират в следните направления: а) приемане на **нов, модерен закон за политическите партии;** б) приемане на специален **закон за финансиране на партиите и на предизборните кампании,** с който да се фиксират точно начините на финансиране, в т.ч. **ограничаване на държавното субсидиране на партиите** за сметка на стимулиране на собствените финансови приходи от партийна дейност; в) **регламентиране на лобизма със специален закон** в държавата, в който ясно да се определят правилата на демократичния политически процес, сиреч легитимните механизми за поддръжка на различните политически субекти от страна на бизнеса, и, разбира се, ролята на партиите в този процес.

8) Ограничаване на политическите привилегии

Това при всички положения е една от най-трудните реформистки мерки поради простата причина, че консуматорите на тези привилегии, т.е. самите действащи политици, трябва да извършат такова народополезно държавническо дело. И все пак няма кой, освен законодателите в различните държави да се „престрашат“ и да направят промени с цяла поредица мерки за драстично „свиване“ на политическите привилегии, а именно: **приемане на специални закони за привилегиите на политиците,** в които на базата на количествени и качествени критерии могат да се ползват държавните благинки, но само за свършена работа; драстично намаляване на сегашните раздути привилегии и свеждането им само до няколко – прилично възнаграждение, служебен транспорт, медицинско обслужване и специална охрана (според длъжността на политиците); извършване на преглед на всички законови и подзаконови нормативни документи (постановления, наредби, правилници), с които са регламентирани привилегиите, и приемане на единен нов правилник за тяхното ползване; **създаване на специализиран контролен орган от експерти на обществени начала,** който да извършва проверки за спазване на клаузите на консумиране на едни или други изгоди и пр., и пр. (Вж. подробната разработка на горните проблеми във: [1: 506 – 521; 2: 357 – 369; 3: 600 – 626.)

9) Коренна промяна във функционирането на службите за сигурност

Тези промяна произтича от самата същност на службите, осигуряващи сигурността на страната, и острата потребност от тяхното отваряне към обществото и от засилване на доверието към тях от хората и държавата. Или, става дума за такава промяна, която засяга дълбоко функционирането на структурите на Министерството на вътрешните работи (МВР), Държавна агенция „Национална сигурност“ (ДАНС), Държавна агенция „Разузнаване“ (ДАР), Държавна агенция „Технически операции“ (ДАТО), Националната служба за охрана (НСО) и др., които решително следва да се реформират в контекста на политическите мерки за демонтиране на ДД.

10) Развитие на свободни и независими медии

Прастара истина е, че свободата на словото е сърцевината на политическата демокрация, поради което само ще рамкираме, че устоите на дълбоката държава успешно могат да бъдат разрушени само ако са налице демократични, свободни и независими медии, изцяло освободени от оковите на българската дълбока държава. В този смисъл най-после е необходимо да бъдат приети **закон за електронните и печатните медии,** закон за българската национална телевизия и радио и др., с които трайно да се утвърдят и наложат демократичните правила и механизми и независимостта на различните медии като юридически фундамент на свободата на словото в борбата с попълзновенията на ДД, целяща завладяване на цялото медийно пространство.

II) Прилагане на непредставителната (пряката) демокрация

Когато говорим за реформиране на политическата система в държавата, едва ли е необходимо да подчертаваме предимствата на обществения избор при **пряката демокрация** като ефективна форма за подбор на професионално подготвени, качествени политици и за рационален контрол при работата на институциите на властта. Тази форма, популярна още и като „референдумна демокрация“ (каквато е в Швейцария), твърде рядко се прилага в масови мащаби по света, защото действително разполага със значителни възможности за ограничаване на всякакво лобистко влияние под напора на парите в политическия процес. Нейното най-голямо предимство е това, че тя в значителна степен елиминира порочните деформации на представителната демокрация, идващи от личната заинтересованост на политиците, понеже различните решения се взимат от гласоподавателите чрез гласуване на всенародни референдуми. По същество такъв демократичен форум за допитване до хората е **вторична и ефикасна форма на контрол върху избраниците на народа, която стопира евентуалното законово прокарване на тясногрупови, егоистични и корпоративни интереси.** Точно тази е и основната причина пряката демокрация неоснователно да се пренебрегва в повечето демократични държави въпреки убеждението на огромното мнозинство хора там, че именно това е бъдещето на едно по-съвършено и по-справедливо народовластие (според авторитетни проучвания на общественото мнение). Естествено, затова е потребно да си приемат съвършено нови и качествени **закони за референдумите,** с които да се гарантират качеството, ефективността и честността на тяхното провеждане (на допитванията до народа).

III) Възраждане на съвещателната демокрация

Съвещателната демокрация е демокрация, при която гражданите не само гласуват за политици, но и разговарят както с тях, така и с различни експерти. Тази демокрация е форма на народовластие, в което колективното обсъждане е централно, а участниците формулират конкретни и рационални решения на обществени предизвикателства на базата на експертната информираност и аргументация и на мненията на хората. За да се избегне ситуация, в която някои напористи участници „превземат“ груповия процес, е препоръчително да се работи с по-малки подгрупи, професионални медиатори и изготвен сценарий [5: 98].

Този тип демокрация е „реанимиран“ от американския учен Джеймс Фишкин, с което се предизвиква истински теоретичен обрат в политическите науки. А това, че съвещателната демокрация – пише Давид ван Рейбрук – може да даде мощен импулс (и наистина го дава) на болезненото тяло на избирателната представителна демокрация, вече почти не буди съмнение у повечето сериозни изследователи. Защото гражданското участие не е само въпрос на участие в протести, стачки, подписване на петиции и други форми на позволена мобилизация в публичното пространство. Напротив, то трябва да бъде и институционално закотвено и гарантирано [5: 100 – 101], за да е ефективно политически. В този контекст съвещателната демокрация може да бъде мощно оръжие за демократизиране на обществото и ограничаване на олигархичните и корпоративните посегателства върху политическата власт.

Изложените възгледи за преодоляване на дълбоката държава и нейното реално демонтиране чрез механизмите на реформите на политическата система, разбира се, не е онова „целебно биле“, което тутакси ще възкреси позалинелите съвременни ценности на демокрацията. За да стане това действително, са необходими още много други, ефективни механизми за усъвършенстване на демократичното развитие на страната, и преди всичко: **нова демократична формула на управление,** друг, **новаторски стил на държавно управление,** както и появата на **нови политически лидери реформатори,** които смело ще приложат посочените реформистки мерки с цел демонтиране един път завинаги на рецидивите на дълбоката държава. По същество реално е необходим **нов, радикален политически (и икономически) преход,** който да засегне абсолютно всички структури в управлението на държавата. Само така може да се преодолее властващата тирания на ДД и решително да се демократизира цялото българско общество.

Промени в службите за сигурност и тяхната демократизация

На фона на развитите възгледи за състоянието на дълбоката държава като уродлив израстък на българската демокрация не е трудно да се досетим, че почти всички служби за сигурност са зависими в една или друга степен от домогванията на агентите на тази държава в работата на цялата система за национална сигурност, и респективно във всички различни органи за сигурност в трите вида власт, т.е. навсякъде в специализираните държавни институции. Това – едно. Друго, не е тайна, че тези служби в зависимост от предназначението си в определени моменти и ситуации изпълняват външна воля и извършват незаконосъобразни дейности, които противоречат на техните правомощия. Тоест изпитват силно давление от агентите за влияние на дълбоката държава, които изобщо не се свенят да се бъркат във важни дела на легитимните държавни институции. В този смисъл ще изложим в синтезиран порядък нашето виждане (от политологическа гледна точка) относно това в каква насока следва да се реформират службите за сигурност, за да са ефективни в борбата срещу оковите на дълбоката държава.

Едно от първите неща, което следва да се направи, е приемане на **доктрина (и стратегия) за националната сигурност** на Република България, която на базата на позитивните демократични образци от Европа ще регламентира цялостно статута, ролята, мястото и функциите на всички органи, свързани със сигурността в държавата (МВР, ДАР, ДАНС, НСО и т.н.).

От особено значение е да бъде обсъден въпросът за приемането на **общ закон** (или подобряване на сегашните отделни закони) **за службите за сигурност,** чрез който тези важни институции и стожери на държавността да заработят още по-ефек-

тивно, да са по-близко до гражданите и да бранят с конституционни средства националните интереси на държавата. В това обновено законодателство следва да се затворят всички вратички за натиск от страна на агентите на дълбоката държава спрямо ключовите държавни институции за сигурността, като по този начин ще се гарантира игнорирането на всевъзможни нелегитимни влияния с политически и други средства.

Друг сериозен проблем пред тези служби, който неизбежно трябва да се решава, е тяхното поетапно **обновление с висококвалифицирани кадри,** с чиито професионални знания и умения действително ще се води решителна битка с представителите на дълбоката държава в името на реда, законността и конституционализма. За целта може да се помисли за откриването на нови специализирани факултети за подготовка на такъв тип кадри (разузнавачи, експерти по сигурност и др.) в специализираните висши училища в страната.

На следващо място е наложително да се **увеличи финансирането на сектор сигурност** в държавата с много повече парични ресурси, които ежегодно да се инвестират в обучение на специалисти, в модернизиране на остарялата база, в закупуване на модерна техника и апаратура и пр., и пр.

И най-накрая спешно трябва да се предприемат **законодателни и всякакви други мерки за рязко ограничаване на възможностите за външно вмешателство в работата на висшите държавни ръководители и службите,** за да се отрежат пипалата на дълбоката държава във всички сектори на националната сигурност. Или, иначе казано, да се сведат до абсолютния минимум сега съществуващата политизация на почти всички важни служби за сигурност в държавата.

* * *

Такива са според нас същността и характеристиката на българската дълбока държава и най-съществените политически и законови мерки, които следва да се предприемат за нейното тотално демонтиране. Дори и само малка част от тях да бъдат реализирани, няма съмнение, че българските институции поне като начало ще се освободят от прангите на дълбоката държава, което ще бъде нов, качествен етап в понататъшното демократизиране на нашата страна.

Литература

1. **Манолов,** Г. Въведение в политическата наука. Пловдив: ВУСИ, 2020.
2. **Манолов,** Г. Цената на изборите, или как партиите си купуват властта. Пловдив: Паисий Хилендарски, 2009.
3. **Манолов,** Г. Власт и привилегии в политическата история (XXX в. пр.н.е. – XXI в. н.е.). Т. III. Пловдив: ВУСИ, 2022.
4. **Начев,** Й. Дълбоката държава. (The deep state.) София: Труд, 2017.
5. **Рейбрук,** Давид ван. Против изборите. София: Сиела, 2020.
6. **Scott,** Peter Dale. The state, the deep state, and the Wall Street Overworld. – In: *The* Asia-Pacific Journal, Japan in Focus, March 3, 2014, Vol. 12, Issue 10, No 5. Updated March 13, 2014. [online]. *http://apjjf.org/2014/12/10/Peter-Dale-Scott/4090/article.html; https://vimeo.com/123052701.*

МИТНИЧЕСКО РАЗУЗНАВАНЕ И РАЗСЛЕДВАНЕ ЗА ИЗПИРАНЕ НА ПАРИ

проф. д-р Атанас Льондев, докторант Тодор Керанов
Висше училище за сигурност и икономика – Пловдив

CUSTOMS INTELLIGENCE AND MONEY LAUNDERING INVESTIGATION

Prof. Atanas Lyondev, PhD, Todor Keranov, PhD student
Higher School of Security and Economics – Plovdiv

Резюме: *Митническото разузнаване и разследване е ключова дейност в системата на митническия контрол, притежаваща специфични цели, които обуславят неговата роля по отношение на превенцията и разкриването на административните нарушения и престъпления срещу митническия, акцизния и валутния режими на страната. Чрез научен и приложен анализ и синтез е направен опит теоретично да се обоснове функционалният модел на митническо разузнаване и разследване, което да даде възможност в практически аспект да бъде изяснена логиката на неговото функциониране в дейността по изпиране на пари.*
Ключови думи: *митническо; разузнаване; разследване; контрол; модел*

Abstract: *Customs intelligence and investigation is a key activity in the customs control system, having specific objectives that determine its role in the prevention and detection of administrative violations and crimes against the country's customs, excise and foreign exchange regimes. Through scientific and applied analysis and synthesis, an attempt has been made to theoretically substantiate the functional model of customs intelligence and investigation, which would enable the logic of its functioning in the money laundering activity to be clarified in a practical aspect.*
Key words: *customs; intelligence; investigation; control; model*

Понятието „изпиране на пари“

Понятието „изпиране на пари“ е относително ново, но тази дейност не е нова. Винаги когато се е появявала необходимост да се скрие финансов трансфер, е възниквало явление, като изпиране на пари. За да изперат парите, генерирани от престъпната си дейност, за перачите е характерно, че имат голямо разнообразие и възможности. Схемата, при която се използва комбинация между банка и бизнес, може да се разглежда като основна за изпиране на пари, а всичко останало се явява нейни варианти. Изпирането на пари е процесът, чрез който престъпниците прикриват незаконния произход на активите си. Те използват нелегални финансови системи, за да обработват трансакции и плащания далече от механизмите за надзор.

В световен мащаб [4: 195] изпирането на пари е между 715 млрд. евро и 1.87 трлн. евро от световния БВП (2 – 5 %) всяка година. В Европейския съюз 70 % от действащите престъпни мрежи упражняват някаква форма на изпиране на пари, за да финансират операциите си и да прикриват активите си; 80 % от престъпните мрежи, действащи в ЕС, използват неправомерно законни бизнес структури за престъпната си дейност; между 117 и 210 млрд. евро са подозрителните дейности и трансакции, извършвани чрез финансовата система и икономиката на ЕС. Но такива числа са малко повече от догадки. Невъзможно е да се каже дали парите се броят за първи или 21-ви път, когато преминават през финансовите центрове. Невъзможно е да се каже

колко пари са успешно изпрани и следователно напълно оставени в сметките. Но какъвто и да е точният обхват, изпирането на пари е огромен проблем за всяка финансова система.

В икономически аспект [3: 32] финансовата система на всяка държава представлява съвкупност от относително обособени парични потоци или финансови отношения, а в институционален план – съвкупност от институции, които регламентират, осъществяват, управляват и контролират финансовите отношения. Последните по своята същност биват два вида – фискални финансови отношения, които обхващат приходите и разходите на държавата (бюджета), и нефискални, изразяващи постъпленията и разходите на юридическите и физическите лица. Обект на посегателство при изпирането на пари могат да бъдат и двата вида финансови отношения. В основата на функционирането на всяка финансово-кредитна система е убедеността на гражданите, че в нея се реализира движение на легално придобити парични потоци, че имат защита на своите бизнес интереси – корпоративни, финансови и др. Изпирането на пари подлага финансовата система на различни рискове – риск за имиджа и добрата репутация, който е най-важният актив на всяка финансова институция.

Теоретичните обобщения и конкретните анализи по отношение на изследвания проблем доказват и аргументират съвременната роля на митниците по отношение на превенцията и противодействието на изпирането на пари като все по-необходимо и оправдано. Тази нова роля на митниците увеличава възможностите за анализ на риска и на конкретните видове рискове и тяхното проявление по отношение на митническия контрол за правилното функциониране, репутация и стабилност на българския бизнес. Необходимо е да се подчертае, че се касае за тенденция, която е свързана с увеличаване на разходите за финансовия и нефинансовия сектор, за свръхрегулации и поставяне на тези сектори и бизнеса в ЕС в много по-неблагоприятна конкурентна среда спрямо останалите региони в света, където не се прилагат толкова стриктни правила в тази област.

За да изясним задачите на всяка една държава, и по-специално на митническите ѝ служби, в превенцията на изпирането на пари, е необходимо, на първо място, да определим вредите от това явление в световен, респективно в национален, мащаб, и на второ – да уточним модела, по който ще измерваме изпирането на пари. По тази причина определени статистически данни, като размерът на сивата икономика и нейното негативно влияние върху растежа, са от важно значение.

Статистическите данни поначало играят съществена роля по отношение на глобалното измерване на явлението изпиране на пари и приходите от трансгранична престъпност. Веднъж известни, мащабът на изпирането на пари и неговите икономически последици дават възможност да бъде измерен и ефектът от превенцията на престъпленията и от мерките на противодействие на това явление. Наблюдава се дори парадокс, при който по-честите и по-строги санкции нямат възпиращ ефект за престъпността, а напротив – водят до по-високи нива на организирана престъпност и на корупция.

Най-сериозните икономически ефекти от изпирането на пари са увеличаване на сивата икономика, нарастване на престъпността и корупцията и незаконните потоци, възпрепятстване на събирането на данъци и намаляване на темповете на икономически растеж. За да се сведат до минимум тези отрицателни последствия, е необходимо да се определи размерът на „изпраните“ средства съобразно икономическите условия и да се идентифицират най-уязвимите аспекти на изпирането на пари в дадена държава.

В различните проучвания и концепции за оценка на изпирането на пари в глобален мащаб се очертават два основни подхода:

- първият подход е чрез измерване на капиталовите потоци, тъй като изпирането на пари предполага движение на капитали между държавите;
- вторият подход е т.нар. „икономически подход“, изразяващ се в измерване на икономически променливи, като данъчни приходи, сива икономика и приходи от престъпна дейност.

При подхода за оценка на изпирането на пари, базиран на движението на капиталовите потоци, трябва да се прави разграничение между незаконни потоци и изтичане на капитали, тъй като последните могат да бъдат както легални, така и от нелегални дейности, докато незаконните потоци са само с престъпен произход и приходите се преместват с цел прикриване. Levi и Reuter [12: 289] отбелязват, че не всички процеси по изпиране на пари изискват международни сделки. Част от приходите от престъпления обикновено се изпират на вътрешния пазар. По този начин изпирането на пари, което изисква международни сделки, ще създаде незаконни капиталови потоци между държавите.

Движението на капитали има за цел паричните средства да се увеличат, докато преместването на незаконните потоци, свързани с изпиране на пари, не е по икономически мотиви [13: 37]. Последните целят да напуснат съответната територия, за да избегнат разкриването им от правоприлагащите органи. Изтичането на капитали се извършва, за да се избегне юрисдикцията, прилагана за капиталов или валутен контрол. В развитието на подхода за оценка на изпирането на пари чрез измерване на капиталовите потоци съществен принцип има концепцията на Бейкър [5: 34]. Според автора повечето незаконни изходящи потоци от развиващите се държави са свързани с изпирането на пари, тъй като приходите от предикатни престъпления (например корупция, трафик на хора и контрабанда) трябва да бъдат отделени от незаконния им произход. Следователно незаконните потоци действат като средство за прехвърляне на приходи от престъпления.

При първия подход за оценка на изпирането на пари, основан на капиталовите потоци, се използват пет основни метода на измерване: методът на „горещите“ пари, остатъчният подход, методът „Дули“, използването на международна търговска система и изчисляването на незаконните финансови потоци.

Методът на „горещите“ пари измерва изтичането на капитали от финансови институции [7: 98]. То се изчислява чрез измерване на потоците на частния капитал, като се вземат грешките, пропуските и частните краткосрочни капиталови сметки от платежния баланс. Този вид изтичане на капитал се определя като „горещи“ пари“, защото възниква като бърз отговор на икономическите условия. Въпреки че този метод първоначално е бил използван за измерване на краткосрочния износ на капитали, той може да бъде приет и за проследяване на незаконните изходящи потоци от приходи от престъпления [11: 178]. Методът на „горещите“ пари търси грешки и пропуски, които отразяват необясними суми, идващи от движението на нерегистрирани капитали, като сделки с офшорни центрове, фалшиви трансакции и подфактуриране. Колкото по-големи са „грешките и пропуските“ в сметките за платежния баланс, толкова по-вероятно е дадена държава да стане жертва на дейности, свързани с изпиране на пари [16: 387].

Остатъчният метод е представен от Kolako и кол. [6: 235] в Доклад за световното развитие от 1985 г. При този подход изтичането на капитали се измерва като сума от брутните притоци н капитали и дефицита по текущата сметка, като се намалява увеличението на официалните валутни резерви. Тук капиталовите потоци се дефинират като сума от промените в брутния вътрешен дълг (публичния и частния) и нетните преки чуждестранни инвестиции.

Методът „Дули“ [8: 90] разглежда изтичането на капитали като компенсиране на вземанията от акции, които не генерират инвестиционен доход и се отчитат в платежния баланс заедно с външния дълг. Дули също така използва изтичането на капитали от сметката на платежния баланс и ги коригира, за да открие нерегистрирани изходящи капитали. За да извърши тези корекции, той разглежда грешките и пропуските, както и промените във външния дълг и международните пазарни лихвени проценти. Неговият подход предполага, че лихвите по законно изтичащите капитали ще бъдат отчетени в платежния баланс, докато лихвата, натрупана върху незаконния капитал, няма да бъде докладвана.

Методът „Използване на международна търговска система“ измерва прехвърлянето на престъпни капитали чрез външнотърговски сделки. Размерът им зависи от стойността на експортните или импортните стоки посредством под- или надфактуриране. Този метод е сред основните начини на прехвърляне на парични средства през граница, използвани от престъпни организации и финансисти на терористи [10]. Специализираната група FATF в доклада си „Trade Based Money Laundering“ посочва, че международната търговия е била използвана от лицата, извършващи изпиране на пари, за прикриване на приходи от престъпления. Изследването определя тази дейност като „процес на прикриване на приходи от престъпления и тяхното преместване чрез използване на търговски сделки в опит да се легитимира незаконният им произход“.

Зданович [18: 854] също анализира незаконните изходящи потоци от САЩ с цел изпиране на пари на основата на международната търговия, като използва несъответствието между данните за износа и вноса от САЩ и държавите партньори за конкретни продукти. Той установява, че някои американски експортни продукти са регистрирани на значително по-ниски цени от световните, докато цените на някои вносни продукти са значително по-високи.

Методът на изследване на капиталовите движения в контекста на размерите на изпирането на пари е използван в проучванията на Глобалната финансова организация (Global Financial integrity-GFI, Washington) за оценка на незаконните потоци от развиващите се държави. Подходът, използван от GFI, е комбинация от метода на некоректното фактуриране в търговските сделки и методът на остатъчните, или „горещите“ пари.

Вторият подход е т.нар. „икономически подход“, изразяващ се в измерване на икономически променливи, като данъчни приходи, сива икономика и приходи от престъпна дейност. Размерът на изпирането на пари се изчислява, освен чрез измерване на капиталови потоци, и чрез оценка на определени икономически променливи, като данъчни приходи, сива икономика и приходи от престъпна дейност.

При този способ за оценка могат да се използват макроикономически показатели (състояние на публичните приходи, данни за престъпността и др.).

Икономическият подход за определяне на мащабите на изпирането на пари включва три основни модела: модел на динамични множествени индикатори (DYNAMIC), динамичен двусекторен модел на равновесие и гравитационен модел на Уолкър.

Моделът на динамични множествени индикатори DYNAMIC е статистически модел на ненаблюдавани (латентни) променливи. Използват се фактори, влияещи върху изпирането на пари (като законодателство, данъчно облагане и др.), и показатели за промени в сивата икономика (например парични показатели, пазар на труда и пазар на продукцията). Този модел свързва ненаблюдаваните променливи с наблюдаваните показатели. Моделът DYNAMIC е приложен от Шнейдър [15: 156] в 145 държави за оценка на сенчестата икономика и размера на изпирането на пари [16: 387].

Динамичният двусекторен модел на равновесие съдържа два сектора – законен и криминален, и двама посредници – фирми и домакинства. Фирмите могат да произвеждат редовни и нередовни стоки, които ще се употребяват от домакинствата. Освен това домакинствата могат да предоставят трудови услуги както на легалния, така и на криминалния сектор. Въпреки това фирмите и домакинствата могат да бъдат използвани от двата сектора за извършване на престъпни дейности и могат да използват законния сектор за прикриване на приходи от престъпници.

Гравитационният модел на Уолкър е разработен от австралийския икономист и криминолог професор Джон Уолкър през 1994 г. и дава възможност да се оценят незаконните финансови потоци между различни световни юрисдикции. Неговата научна методология съчетава познания от криминологията, икономиката и финансите. Теоретичната основа на модела е универсалният закон за гравитацията на Нютон, разработен през 1687 г., съгласно който силата на привличане между два обекта зависи от тяхната маса, разстоянието между тях и гравитационната константа. Според модела на привличане на Уолкър незаконните финансови потоци между две държави, подобно на търговските сделки, зависят от „икономическата тежест“ на тези държави (измерена като брутен вътрешен продукт – БВП), физическото (географското) разстояние и общите езикови и културни връзки между тях. Уолкър описва своя теоретичен модел, като свързва изпирането на пари с доходите на лицата, получени от различни престъпления.

Гравитационният модел е използван първоначално от Уолкър и Австралийския център за финансово разузнаване за измерване на изпирането на пари в Австралия, а по-късно е доразвит в проучването на Уолкър и Унгер [17: 78] за количественото определяне на изпирането на пари в световен мащаб. Т.нар. „модел на привлекателност“ на Уолкър и Унгер се основава на оценка на различните видове престъпления в дадена държава, произтичащите от тях доходи и прогнозния дял на средствата, които ще бъдат изпирани във и извън страната. Определят се „привлекателни“ държави за изпиране на средства чрез индекс, който разчита на фактори като възможности и рискове, представени от финансовите институции в дадена държава.

Службата на ООН по наркотици и престъпност (United Nations Office on drugs and Crime – UNODOC) също използва гравитационния модел за измерване на изпирането на пари от приходите от наркотрафик и трансгранични престъпления. Изчисленията на международните престъпления се базират на четири въпроса: колко са извършените престъпления; каква е печалбата от тях; каква част от печалбата се изпира; и къде се извършва изпирането [14: 51]. Използват се също параметрите за привличане на Уолкър и Унгер, които са модифицирани: БВП на глава от населението; значението на сектора на финансовите услуги в БВП (износът на финансови услуги като процент от БВП); притокът на преки чуждестранни инвестиции като процент от БВП; индекси, измерващи върховенството на закона (показател за върховенството на закона); индекси, измерващи човешкото развитие; делът на сивата икономика и др.

Гравитационният модел е използван и в Проект за икономическата и правната ефективност на политиката за борба с изпирането на пари и борбата с финансирането на тероризма [9: 96], финансиран от Европейската комисия. За разлика от доклада на UNODOC, който измерва изпирането на пари основно от наркотрафик, докладът на Европейската комисия измерва легализирането на средства от множество източници, включително трафик на хора, престъпления срещу околната среда, измами, кражби на автомобили, грабеж и изнудване и убийство и заплаха за убийство, включително отвличане за откуп, фалшиви лекарства и контрабанда на алкохол и тютюневи изделия. ECOLEF [9: 96] класифицира индекса на привлекателност в

три групи: БВП на глава от населението; значението на сектора на финансовите услуги в БВП (износът на финансови услуги като процент от БВП); и индексът за „комбинирано изпиране на пари“. Последният индекс се изчислява, като се използват две предположения: способността на държавата за противодействие на изпирането на пари; и възможностите за такава дейност.

В обобщение се налага изводът, че съществуват множество способи за измерване на мащабите на глобалното изпиране на пари. Като най-ефективни обаче се налагат два основни подхода: чрез измерване на капиталовите потоци и чрез измерване на икономически променливи. Въпреки това няма абсолютен подход или универсален модел, който да описва точното състояние във всяка държава. Всеки модел има известни слабости и недостатъци. Независимо от несъвършенствата и липсата на абсолютни доказателства за значимостта на изпирането на пари, определяйки го като негативно влияние, то носи крупни загуби за всяка икономика поотделно и в световен мащаб.

Ролята на митническите органи в изпирането на пари

Изпирането на пари и противодействието му в световен, регионален и национален мащаб е предмет на изследвания от учени и експерти в областта на наказателното право, криминологията, криминалистиката, теорията на оперативно-издирвателната дейност.

Ролята на митническите органи е от ключово значение за предотвратяване на незаконни финансови потоци и осигуряване на финансовата сигурност. Необходима е промяна в митническите дейности, като част от мерките за изваждане на Република България от т.нар. „сив списък“ на държавите под засилено наблюдение за изпиране на пари. Значима е мотивацията от страна не само на митническите органи, но и на бизнес средите, като анализ и управление на риска за „изсветляване“ на процеса на изпиране на пари и защита на финансовата сигурност от митниците, като принос и мярка за изваждане на България от този списък.

Митниците придобиха първостепенно значение за защита на финансовите интереси на ЕС и осигуряване на финансовата сигурност, като изпълняват съществена роля в превенцията и противодействието на изпирането на пари, свързано с контрола на паричните средства, преминаващи през вътрешната и външната граница на Съюза. Необходимостта да се разгледа подобна тема в доклад произтича от промените, настъпили в европейската правна рамка, регламентираща внасянето и изнасянето на парични средства през границите на Европейския съюз, както и правомощията, възложени на митническите органи при упражняване на валутен контрол [2].

Дирекция „Митническо разузнаване и разследване“ е част от организационната структура на централното митническо управление на Агенция „Митници“ – ръководи и участва в митническата дейност, свързана с разузнаването и разследването на административни нарушения, респ. престъпления, които са от компетентността на митническите органи, чрез извършване на контролни действия за противодействие и разследване на незаконно пренасяните през държавната граница парични средства, благородни метали, скъпоценни камъни и изделия със и от тях [2]. За изпълнение на тези действия се осъществяват взаимодействие и обмен на информация с правоохранителните и правоприлагащите органи в областта на разузнаването и разследването на административните нарушения/престъпления от компетентността на митническите органи.

Основната цел на Дирекцията е да осъществява с успех задачи, свързани с осъществяване на митническо разследване и извършване на неотложни действия, когато

това се налага, за да могат да се събират качествени доказателства по дела за митнически престъпления. При изпълнение на служебните задължения на митническите служители са необходими специализирани знания и създадени умения както в областта на досъдебното производство, така и в сферата на модерните административни, информационни и мениджърски техники, във връзка с дейността на Министерството на финансите и Агенция „Митници“.

Митническо разузнаване и разследване

От приемане на Република България в Европейския съюз през 2007 г. до този момент митническото разузнаване и разследване като дейности в системата на митническия контрол са се развивали в организационен аспект основно чрез два структурни модела – децентрализиран (от 2007 г. до 7.01.2019 г.) и централизиран (от 7.01.2019 г. до момента). И двата модела са със силноизразени характеристики, полярно разположени по отношение на изградени структури, йерархична подчиненост и териториално разположение. Както единият, така и другият модел има съответни предимства и недостатъци. В тази част на изложението на основата на практикоприложен анализ ще бъдат разгледани организационните модели на МРР от гледна точка на техните предимства и недостатъци. От 2007 г. до 7.01.2019 г. организационният модел на МРР се е основавал на разбирането за значителна децентрализация в структурно отношение. Моделът на организация на митническото разузнаване и разследване към настоящия момент може да бъде описан по следния начин: Дирекция „Митническо разузнаване и разследване“ е част от специализираната администрация на централното митническо управление на Агенцията. Дирекцията се ръководи от директор, който може да се подпомага от заместник-директори. Дирекцията е организирана в териториални звена, отдели, сектори и други звена от по-нисък ранг. Териториалните звена на Дирекция „Митническо разузнаване и разследване“ са териториални отдели, които са под ръководството на директора в Дирекция „МРР“ и не се включват в структурата на териториалните дирекции. Териториалните отдели на Дирекция „Митническо разузнаване и разследване“ се ръководят от началник, който ръководи пряко и дейността на съответния териториален отдел. Функциите, дейността и задачите на териториалните отдели на Дирекция „Митническо разузнаване и разследване“ се определят и утвърждават от директора на Агенцията. Така създаденият организационен модел на митническото разузнаване и разследване е силно централизиран, до известна степен действащ самостоятелно.

Могат да се очертаят следните негови предимства:

✓ експресна и точна комуникация между възложител и изпълнител на задачи от областта на МРР;

✓ ограничаване на възможностите за нерегламентирано изтичане на информация;

✓ добър контрол и координация на териториалните отдели в национален план;

✓ уеднаквяване и повсеместно въвеждане на добрите практики.

Този модел крие и някои съществени недостатъци, които са следствие от силно централизираната система на митническото разузнаване и разследване, а именно:

✓ прекъсване на непосредствената работна връзка с колеги от други отдели на специализираната администрация – води до загуба на важна и актуална информация, получавана в реално време;

✓ постепенна загуба на професионална компетентност по отношение на нови и специфични моменти в митническото и акцизното законодателство;

✓ значителна степен на затруднение в екипната работа между служителите на МРР и останалите структури на специализираната администрация;

✓ липса на конкуренция между структурите на МРР и другите звена от специализираната администрация по отношение на разкриването на нарушения и престъпления.

Този модел на действащата към момента организационна структура на МРР е със силно централизиран характер и значителна самостоятелност при изпълнение на оперативните дейности. В момента началниците на териториални отдели МРР са подчинени пряко на директора на Дирекция „МРР“. Определянето на задачи, контролът по изпълнението им и оценяването на дейността на всички звена от структурата на Дирекция „МРР“ се извършват от директора. Информационният поток по отношение на разузнавателна информация се движи в основни линии между териториалните отдели и Дирекция „МРР“, което поставя в известна степен на изолираност останалите структурни звена в териториалните митници по отношение на изпълнението на оперативните им дейности.

Като обобщение на казаното може да се посочи, че и двата модела имат своите предимства и недостатъци, а придобитият опит показва, че при преминаване от една крайност в друга в организацията на работа и структура в дейността по митническо разузнаване и разследване постигането на оптимални резултати ще бъде значително затруднено. Недостатъците са носители на рискове по отношение на обмена на информация, комуникацията, координацията и сътрудничеството в рамките на прилагане на европейските политики при митническия контрол.

В резюме на разгледаните дотук въпроси, свързани с целите, ролята, функционалните и организационните аспекти на митническото разузнаване и разследване, могат да се направят следните обобщения:

Първо. Изведена е позицията, че митническото разузнаване и разследване е ключова дейност в системата на митническия контрол, притежаваща специфични цели, които обуславят неговата роля по отношение на превенцията и разкриването на административните нарушения и престъпления срещу митническия, акцизния и валутния режим на страната.

Второ. В рамките на изследването чрез научен и приложен анализ и синтез е направен опит теоретично да се обоснове функционалният модел на МРР, което да даде възможност в практически аспект да бъде изяснена логиката на неговото функциониране в дейността по изпиране на пари.

Трето. На основата на практикоприложен анализ са разгледани двата модела за организационно структуриране на МРР, действали през периода след приемането на страната ни в Европейския съюз. Изведените ключови аспекти от организационно естество при двата модела могат да послужат за основа при по-нататъшен задълбочен анализ на основните им предимства и недостатъци.

Литература

1. **Агенция** Митници. [онлайн]. [прегледан 2.03.2025]. *https://customs.bg/.*
2. **Валутен** закон. [онлайн]. [прегледан 11.03.2025]. *https://lex.bg/laws/ldoc/-12802047.*
3. **Касова,** Е. Здравната сигурност като част от сигурността на страната. – В: *Национална* сигурност, бр. 17, 2024, с. 32.
4. **Радев,** Е. Мерките срещу прането на пари в Европейския съюз – реформа в ход. – В: *Известия* на Икономически университет – Варна, бр. 3, 2020, с. 195.
5. **Baker,** R. Capitalism`s achilles heel: Dirty money and how to Renew the Free-Market System. Hoken, NJ: Wiley, 2005, p. 34.
6. **Colaco,** F., and al. World Development Report. Washington, DC: The World Bank, 1985, p. 235. [online]. *htpp://documents.worldbank.org/curated/en/1985/01/17390599.*

7. **Cuddington,** J. Capital Flight: Estimates, Issues, and Explanations. International Finance Section, department of Economics, Princeton University Princeton, NJ, 1986, p. 98.
8. **Dooley,** M. Country specific risk premiums, capital flight and net investment income payments in selected developing countries. IMF Departmental Memorandum, 1986, p. 90.
9. **ECOLEF.** The Economic and Legal Effectiveness of Anti Money Laundering and Combating Terrorist Financing Policy (ECOLEF). JLS/2009/ISEC/AG/087. Utrecht University, European Commission, Directorate-General (DG) Home Affairs, 2013, p. 96.
10. **FATF.** Trade Based Money Laundering. Paris: Financial Action Task Force. [online]. [available 23.02.2025]. *https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoney-laundering.html.*
11. **Kar,** D. and B. LeBlanc. Illicit Financial Flows to and from the Philippines: A Study in Dynamic Simulation, 1960-2011. – In: *Global* Financial Integrity, 2014, p. 178.
12. **Levi,** M. and P. Reuter. Money laundering. – In: *Crime* and Justice, Vol. 34, No. 1, 2006, p. 289.
13. **Macskiming,** S. Trade based money laundering: responding to an emerging threat. – In: *Deakin* Law Review, Vol. 15, No. 1, p. 37.
14. **Pietschmann,** T. and J. Walker. Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crime. Research Report. United Nations Office on drugs and Crime (UNODOC), 2011, p. 51.
15. **Schneider,** F. Shadow economies and corruption all over the world: what do we really know? – In: *Working* paper, No. 0167, 2006, p. 156.
16. **Schneider,** F. and U. Windischbauer. Money laundering: some facts. – In: *European* Journal of Law and Economics, Vol. 26, No. 3, 2008, p. 387.
17. **Walker,** J. and B. Unger. Measuring global money laundering: the walker gravity model. – In: *Review* of Law & Economics, Vol. 5, No. 2, 2009, p. 78.
18. **Zdanowicz,** J. Trade based money laundering and terrorist financing. – In: *Review* of Law and Economics, Vol. 26, No. 5, 2009, p. 854.

ИЗКУСТВЕН ИНТЕЛЕКТ В ЕКОСИСТЕМАТА НА СИГУРНОСТТА

проф. д.н. Николай Радулов
Нов български университет – София

ARTIFICIAL INTELLIGENCE IN THE SECURITY ECOSYSTEM

Prof. Nikolay Radulov, DSc
New Bulgarian University – Sofia

Резюме: *Изследва се ролята на изкуствения интелект (ИИ) в контекста на Сигурност 5.0, като се анализират трансформацията на класическите методи за сигурност и появата на нови дигитални предизвикателства. Фокусът е върху интеграцията на ИИ в дейностите по обезпечаване на сигурност.*

Ключови думи: *изкуствен интелект; киберсигурност; разузнаване; контраразузнаване; мрежи; прогностичен анализ; предикативност; блокчейн; екосистема; хибриден*

Abstract: *The study examines artificial intelligence's (AI) role in the context of Security 5.0, analyzing the transformation of classical security methods and the emergence of new digital challenges. The focus lies on AI integration within security assurance activities.*

Key words: *artificial intelligence; cybersecurity; intelligence; counterintelligence; networks; predictive analysis; predictiveness; blockchain; ecosystem; hybrid*

Увод

Технологичният напредък в рамките на Сигурност 5.0 [4] създава нова парадигма в сигурността, чиято същност е в интеграция между физическата и киберсигурността, автоматизацията на процесите за анализ и реакция, проактивния и превантивния подход към заплахите, както и използването на големи данни и прогностичния анализ.

Основни направления на използване

Таблица 1. **Ключови приложения на ИИ в сигурността**

Направление	Технологично решение	Очаквани резултати
Киберсигурност	Автоматизирано откриване на заплахи	Намаляване на времето за реакция с 60 %
Физическа сигурност	Интелигентно видеонаблюдение	Повишаване на точността на детекция до 95 %
Разузнаване	Анализ на големи данни	Подобряване на прогностичните способности
Контраразузнаване	Поведенчески анализ	Ранно откриване на заплахи

Технологични иновации – ключови технологични компоненти в екосистемата са: дълбоко машинно обучение; невронни мрежи; компютърно зрение; обработка на естествен език; биометрична идентификация.

Предизвикателства и рискове

Таблица 2. **Анализ на рисковете**

Риск	Вероятност	Въздействие	Мерки за намаляване
Нарушаване на лични данни	Висока	Критично	Усъвършенствани криптографски протоколи
Злоупотреба с ИИ	Средна	Високо	Многослойни системи за контрол
Технически проблеми	Ниска	Средно	Резервни системи и процедури

Бъдещи тенденции – очакваните развития са в посока на: квантови изчисления в криптографията; разширена реалност в наблюдението; интегрирани биометрични системи; автономни системи за реакция.

Таблица 3. **Прогнозни тенденции 2025 – 2030**

Технология	Очаквано въздействие	Времева рамка
Квантови компютри	Революционно	2028 – 2030
Невроморфни чипове	Значително	2026 – 2027
6G комуникации	Високо	2027 – 2029

Интеграцията на ИИ в системите за сигурност представлява фундаментална промяна в подхода към защитата на обществените интереси. Успешното внедряване изисква балансиран подход между технологии и етика, непрекъснато обучение на специалисти, международно сътрудничество и гъвкава регулаторна рамка.

Приложения на изкуствения интелект в службите за сигурност

Киберконтраразузнаване и разузнаване

Анализ на мрежови модели: Darktrace [14] използва алгоритми за *машинно самообучение* за откриване на аномалии в мрежовия трафик, идентифицирайки скрити кибератаки с 95 % точност. Системата прави *профилиране* на цялата мрежа, за да засече непознати шаблони (напр. Command-and-Control трафик); IoT защита – ИИ системи сканират 1M + IoT устройства за уязвимости, използвайки *невронни мрежи,* с 30 % по-бързо от човешки анализатори. *Пример:* Устройства за умни къщи могат автоматично да блокират подозрителни API заявки към облачни сървъри.

Физическо наблюдение. Лицево разпознаване: системата Ntech Lab [3] идентифицира лица от 200 M архивни снимки с точност 99.7 %, интегрирайки се със системите за видеоанализ на системите на метрото. Идентифицира издирвани лица дори при маскиране.

Предикативно патрулиране: В Лондон PredPol[1] предсказва *горещи точки* за криминална дейност, след като анализира 10K + социоикономически параметри. Намалява престъпленията с 34 % в зони с висок риск.

[1] Предсказуема полиция е използването на математика, предсказуем анализ и други аналитични техники в правоприлагането за идентифициране на потенциална престъпна дейност [6].

Анализ на достъпни източници (OSINT)

Социални мрежи – Платформата Palantir Gotham[2] сканира 10M поста на ден на над 150 езика, откривайки криптографски следи (напр. метаданни в Telegram); лексикални маркери за екстремизъм (думи, като „Аллах Акбар“ в специфичен контекст); финансови следи – Chainalysis проследява $500B криптотрансакции годишно чрез графични невронни мрежи, откривайки прането на пари и свързани портфейли между терористични групи.

Криптоанализ (SIGINT)[3] – Динамично дешифриране – нова генерация алгоритми дешифрират AES-256 за 20 минути вместо 1M+ години, използвайки *квантово-резонантни модели*. Приложими за: Тъмен мрежов трафик (Tor, I2P); Енд-ту-енд шифрирани съобщения (Signal, WhatsApp). *Пример:* През 2022 г. ИИ на NSA декриптира 200TB комуникации с групировки, свързани с Русия.

Геопространствен анализ (GEOINT) – Сателитен мониторинг – Black Sky[4] обработва над 1000HD снимки на час, използвайки *конволюционна невронна мрежа (CNN)* – **регулиран тип невронна мрежа с предварителна връзка,** която получава функции чрез оптимизация на филтър (или ядро), за откриване на: строежи на подземни съоръжения (промени във флората и терена); необичаен трафик на военна техника (+80 % точност спрямо стандартен анализ). *Пример:* Предизвикателството за Азербайджан през 2023 г. – ИИ засича складиране на ракети край границата с Армения 3 дни преди военни действия.

Биометричен анализ – Радиолокационна биометрия. Системи, като Biometrica, използват сензори на милиметрови вълни за: откриване на оръжия под дрехи с 97 % прецизност; идентифициране на физиологичен стрес (пулс, кръвно налягане).

Противодействие на AI заплахи – Deepfake неутрализация. Microsoft Video Authenticator сканира 500 кадъра/сек за: нереални сенки в очите; несъответствия на светлината; *Генеративни враждебни мрежи* (GANs). Ефективност: разкрива фалшиви видеозаписи със 74 % още през предпроцесинга.

Роля на предикативния анализ в контраразузнаването и разузнаването

Предикативният анализ играе преобразяваща роля в съвременното разузнаване и контраразузнаване, комбинирайки исторически данни, машинно обучение и статистически модели на прогнозиране, предотвратяване и неутрализиране на заплахи. Ето ключовите аспекти на нейното приложение:

Прогнозиране на шпионски дейности: моделиране на поведенчески шаблони – анализират се комуникационен трафик, трансакции и социални взаимодействия за откриване на аномалии. *Пример*: Системи, като XKeyscore[5], обработват метаданни от имейли и социални мрежи, за да идентифицират скрити връзки между подозрителни субекти; идентифициране на „спящи агенти“.

---

[2] PalantirGotham е корпоративна платформа за планиране на мисии и провеждане на разследвания, като се използват различни данни, като същевременно се поддържа поверителност и контрол на достъпа [13].

[3] Сигнално разузнаване (SIGINT) е актът и полето за събиране на разузнавателна информация чрез прихващане на *сигнали*, независимо дали става дума за комуникация между хора или от електронни сигнали, които не се използват пряко в комуникацията [7].

[4] Най-модерната космическа разузнавателна платформа в света, предоставяща сателитни изображения, анализи и високочестотен мониторинг [12].

[5] XKeyscore (XKEYSCORE, или XKS) е секретна компютърна система, използвана от Агенцията за национална сигурност на Съединените щати (NSA) за търсене и анализ на глобални интернет данни, които тя събира в реално време [8].

Оптимизация на ресурсите: предикативните модели помагат за разпределяне на патрули в райони с висок риск (напр. близо до критична инфраструктура); приоритизиране на разследванията въз основа на вероятността от сериозни последици.

Киберсигурност. Прогнозиране на кибератаки: Модели за Machinelearning съпоставят мрежови аномалии с исторически шаблони на атаки. *Пример*: Darktrace открива APT (AdvancedPersistentThreat)[6] атаки 48 часа преди ескалация; анализ на darknet за ранни сигнали – алгоритми сканират 10,000+ торент форума дневно за употреба на ключови думи.

Финансово проследяване. Предикативният анализ разпознава: необичайни парични потоци (напр. внезапни трансакции към офшорни райони); криптовалутни преводи към сметки, свързани с чужди разузнавателни служби. *Пример:* Chainalysis [1] проследява $2.3 млрд. криптотрансакции на севернокорейски хакерски групи (2023).

Важно е тук да изясним същността на блокчейн разузнаването. То се развива чрез интеграцията на изкуствен интелект (ИИ) и блокчейн технологии, създавайки изпълнителен слой за Web3 ИИ, който премахва бариерите между изкуствения интелект и блокчейн мрежите.

Основните аспекти включват: безопасност и поверителност – ключова характеристика е използването на технологията Trusted Execution Environment (TEE), която гарантира поверителността и целостността на данните по време на изчисления. Това представлява напредък в сравнение с други решения, които се борят с проблеми, свързани с поверителността и сигурността; интеграция на ИИ – договорите за ИИ агенти (AI-Agentcontracts) имат за цел да направят разполагането на ИИ агенти толкова лесно, колкото изпълнението на умни договори (smartcontracts). Тези договори позволяват динамично управление и контрол на достъпа на ИИ агенти, като привнасят ново ниво на сложност в платформите за обмен на цифрови валути.

Системата предлага впечатляващи интеграционни възможности, включително: възможност за събиране на данни от външни API; интеграция на персонализирани ИИ агенти, включително напреднали езикови модели, като GPT-4; поддръжка на множество ИИ агенти, които могат да си сътрудничат свободно върху сложни приложения в защитени TEE граници. Тази функционалност значително опростява достъпа до децентрализирани приложения и предоставя на разработчиците богати инструменти.

Блокчейн разузнаването разширява границите на сливането на ИИ и блокчейн, като предлага платформа, която подкрепя децентрализирана интелигентност за бъдещето, която гарантира сигурност и неманипулируемост на данните [2: 55]. Напредналата система с множество доказателства (multi-proofnetworksystem) и договорите за ИИ агенти са иновативни функции, които могат да трансформират екосистемата.

Таблица 4. **Ползи от интеграцията на блокчейн и AI**

Аспект	Блокчейн	Изкуствен интелект	Комбиниран ефект
Сигурност	Неизменяемост и автентичност	Анализ на заплахи	Гарантирана цялост на данните
Прецизност	Прозрачен одитен запис	Предикативни модели	Висока точност и достоверност
Скорост	Достъп до всички участници в мрежата	Реално време	Бърз обмен и анализ на информация

[6] Усъвършенствана постоянна заплаха (APT) е скрита или прикрита кибератака. По време на APT лошите участници получават неоторизиран достъп до мрежа, като избягват откриването за продължителен период от време.

Интеграцията на блокчейн и изкуствен интелект в сигурността създава нова парадигма за защита, която комбинира висока сигурност с интелигентен анализ. Комбинацията от непроменимост, проследимост и предикативна сила прави тази технология незаменима в съвременното контраразузнаване и киберсигурност.

Профилиране на заплахи. Създават се динамични профили за: чуждестранни агенти – анализ на академични среди и индустриални конференции за потенциални цели за вербуване; организации с висок риск – оценка на уязвимостите във фирми от стратегически сектори (енергетика, отбрана). *Пример:* През 2022 г. френската DGSE предотвратява опит за кражба на ядрени технологии, използвайки предупредителни сигнали от AI модел, анализиращ CV-тата на изследователи.

Предикативният анализ е мощен мултипликатор в контраразузнаването, но изисква баланс между технологичната мощ и етическите ограничения. Очаква се до 2028 г. 75 % от контраразузнавателните операции да интегрират квантово базирани предсказващи модели за обработка на ексабайт[7] данни в реално време.

Примери за успешно използване на ИИ в екосистемата на сигурност по света

САЩ: Интеграция на AI в националната сигурност

Използва се програма **Palantir**[8] (CIA и NSA). Технологии: използване на графови невронни мрежи за картографиране на връзки между заподозрени; прилагане на NLP алгоритми за анализ на метаданни от над 100M имейла дневно. Налице е ключов успех – разкриване на китайска шпионска мрежа през 2021 г., фокусирана върху кражба на данни за полупроводници: ИИ алгоритми откриват необичаен DNS трафик от научни лаборатории. Статистиката сочи: 83 % намаление на успешни кибератаки след внедряването.

Програма **Einstein** (DHS). Функционалност на програмата: мониторинг на 200TB мрежов трафик на ден към федерални агенции; прогнозиране на SQLi атаки[9] с 87 % точност. Документиран случай на пресичане – предотвратяване на криптоджакинг атака[10] срещу системата за управление на въздушен трафик през 2022 г.

Великобритания: Предикативни модели на хибридни заплахи

Използване на **системата HawkEye** [9] (MI5). Технически характеристики: анализ на над 300 000 социални поста на час на над 50 езика. 3D геопространствено картографиране на горещи точки. Резултати: идентифициране на 14 терористични клетки през 2023 г.; намаляване на фалшивите новини с 67 % чрез системи за филтриране на дезинформация.

---

[7] Един петабайт е равен на 1024 TB (терабайта), а един ексабайт – на1 млн. терабайта.

[8] Palantir Technologies предлага набор от софтуерни приложения за интегриране, визуализиране и анализиране на информация. Софтуерът на Palantir се използва в много важни разузнавателни, правоприлагащи, финансови, здравни и отбранителни организации по света. Софтуерът представлява пресечна точка на данни, технологии и човешки опит [10].

[9] SQL инжекцията е най-често използваната атака на нападателя да пробие сигурността на дадено уебприложение. От статистическите данни, които са регистрирани през последните години, става ясно, че SQL инжекцията е най-сериозният и най-вече използван вид кибератака, извършван в сравнение с други атаки [5].

[10] Криптоджакингът е вид киберпрестъпление, което включва неоторизирано използване на устройства (компютри, смартфони, таблети или дори сървъри) от нападатели за копаене на криптовалута [11].

Операция CLOAK (GCHQ)[11]. Използвана иновация: използване на подсилено обучение за симулиране на лъжливи киберследи. *Пример:* Дезинформационна кампания срещу руски хакери (2022), насочена към измама за „сигурни канали“.

Израел: Иновации в киберконтраразузнаването

Технология Pegasus 2.0[12] (NSO Group). Функции: мониторинг на над 50 000 IoT устройства (умни часовници, лампови сензори); откриване на подозрителни Bluetooth свръзки с точност 92 %. Успешно приложение: предотвратяване на хакерска атака срещу водоснабдителната инфраструктура (2020) – ИИ засича аномален трафик от умни водомери към **белоруски сървъри.**

Програма „IronLogic“. Специфика на действие: система за анализ на шифриран жаргон в чат платформи (напр. Telegram); разпознаване на геотагове в Base64 код с точност 89 %.

Франция: Защита на критична инфраструктура

ANSSI AI Threat Intelligence[13]**.** Технологии: използване на самообучаващи се алгоритми за сигнатури от MITER ATT&CK рамката; компютърно зрение за анализ на сателитни снимки за подозрителни обекти. Успешен случай (2022): откриване на скрит компресионен шум в енергийни мрежи, индикация за хакване на SCADA системи.

Операция Astaroth. Реализация: използване на ИИ анализ на кодови фрагменти в GitHub, свързани с руски групировки; следене на 1.2M депозитори за експлойти за критични системи.

Сингапур: Политика против дезинформация

Програма POLARIS (IMDA). Механизми на използване – динамична класификация на фалшиви видеа чрез AI анализ на микромимики и аудиоартефакти. Идентифициране на над 400 координирани кампании (2023). Резултати от използването: намаляване на viral обхвата на фалшиви новини с 75 %.

Таблица 5. **Национални подходи**

Държава	Програма	Технология	Успех	Точност
САЩ	Palantir	Графови мрежи	80 % ↓ кибератаки (2021 – 2023)	94 %
Израел	IronLogic	NLP + GPS анализ	92 % откриване на хибридни заплахи	89 %
Сингапур	POLARIS	Видеоанализ	75 % ↓ дезинформация	91 %
Великобритания	HawkEye	Геопредикция	14 неутрализирани терористични клетки	88 %

Заключение

От извършения анализ стигаме до задълбочени изводи за приложението на изкуствения интелект (ИИ), като основните могат да се обобщят в следните ключови направления:

[11] GCHQ – правителствената агенция за мониторинг е разработила шпионски програми, които дистанционно отвличат камерите и микрофоните на компютрите [15].
[12] Инструмент за наблюдение за Android и iOS [16].
[13] ACN се присъединява към инициативата на високо ниво относно рисковете от ИИ, насърчавана от френската киберагенция ANSSI [17].

Технологична трансформация – интеграция между физическа и киберсигурност; автоматизация на процесите на анализ и реакция; внедряване на проактивен и превантивен подход.

Ключови постижения – повишаване на точността на детекция до 95 % при физическа сигурност; намаляване на времето за реакция с 60 % в киберсигурността; значително подобряване на прогностичните способности.

Иновативни приложения – развитие на дълбоко машинно обучение; усъвършенстване на биометричната идентификация; интегриране на невронни мрежи и компютърно зрение.

Предизвикателства: налични са високи рискове за нарушаване на лични данни; съществува потенциал за злоупотреба с ИИ технологиите; налице е необходимост от многослойни системи за контрол.

Перспективи: съществува процес на развитие на квантови изчисления в криптографията; възможно е интегриране на разширена реалност в системите за наблюдение; реално съществува възможност за създаване на по-автономни системи за реакция.

В екосистемата на Сигурност 5.0 ИИ се превръща във водещ и критичен компонент на модерната екосистема за сигурност, като същевременно поставя важни въпроси относно баланса между технологичен напредък и етични съображения в контекста на националната сигурност.

Литература

1. **Блокчейн** разузнаване за разследвания, риск и сигурност. [онлайн]. *https://www.chainalysis.com/*
2. **Личева,** Т. Сигурност на данните. – В: *Сборник* с доклади от XII Международна научна конференция „Техника. Технологии. Образование. Сигурност“, 2 – 5.09.2024 г., с. 55. ISSN 2535-0323.
3. **Платформа** за многообектен видеоанализ. [онлайн]. *https://ntechlab.com/*
4. **Радулов,** Н. Сигурност 4.0. София: Научно-технически съюз по машиностроене „Индустрия 4.0“, 2019. ISBN 978-619-7383-15-7.
5. *https://ehu.bg/courses/sql-injection/*
6. *https://en.wikipedia.org/wiki/Predictive_policing*
7. *https://en.wikipedia.org/wiki/Signals_intelligence*
8. *https://en.wikipedia.org/wiki/XKeyscore*
9. *https://en.wikipedia.org/wiki/Hawk-Eye*
10. *https://finder.startupnationcentral.org/mnc_page/palantir*
11. *https://www.kaspersky.ru/resource-center/definitions/what-is-cryptojacking*
12. *https://www.blacksky.com/*
13. *https://www.palantir.com/platforms/gotham/*
14. *https://www.darktrace.com/*
15. *https://www.theguardian.com/uk-news/2014/may/13/gchq-spy-malware-programme-legal-challenge-privacy-international*
16. *https://www.safemykid.com/lp/phone-monitoring.html*
17. *https://www.acn.gov.it/portale/en/w/acn-aderisce-ad-iniziativa-di-alto-livello-sui-rischi-dell-ia-promossa-dall-agenzia-cyber-francese-anssi*

КОСМОСЪТ КАТО СРЕДА ЗА ВОЕННИ ОПЕРАЦИИ

проф. д-р Пламен Богданов
Университет по библиотекознание и информационни науки – София

SPACE AS AN ENVIRONMENT FOR MILITARY OPERATIONS

Prof. Plamen Bogdanov, PhD
University of Library Studies and Information Technologies – Sofia

Резюме: *В доклада се изследва използването на Космоса за военни цели от 50-те години на XX век до 20-те години на XXI век. Анализирано е развитието на технологиите за водене на военни дейности и провеждане на военни операции в Космоса, от Космоса и чрез Космоса. Направен е изводът, че днес Космосът се е превърнал в потенциално бойно пространство.*
Ключови думи: *космос; технологии; военно-космически системи; противокосмически комплекс; противокосмическа отбрана*

Abstract: *The paper examines the use of space for military purposes from the 1950s to the 2020s. It analyzes the development of technologies for conducting military activities and conducting military operations in space, from space, and through space. The conclusion is made that today Space has become a potential battle space.*
Key words: *Space; technologies; military space systems; anti-space complex; anti-space defense*

Увод

През 1957 г. Съветският съюз изстрелва първия изкуствен спътник на Земята „Спутник“. Това е ключово събитие в човешката история. Събитието обаче бележи нов етап във военната надпревара между двете суперсили САЩ и СССР по време на Студената война. Изстрелването на първия изкуствен спътник и извеждането му на орбита в Космоса показва, че СССР е разработил технология за производство на мощни балистични ракети, а те могат да носят и ядрени бойни глави. В САЩ това предизвиква сериозни тревоги.

След като през 1958 г. Съединените щати изстрелват първия си сателит „Explorer 1“, постепенно Космосът започва да се използва все по-широко за военни цели.

Използване на Космоса за военни цели по време на Студената война

Анализът на броя и решаваните задачи от ИСЗ, изведени и функциониращи в орбита през първите три десетилетия от космическата ера (1957 – 1987), показва, че около две трети от тях са с военно предназначение. Така едновременно със създаването на първите космически системи възникват и военно-космическите системи (ВКС). Под „ВКС“ се разбира съвкупност от функционално взаимносвързани и съгласувано действащи средства с космическо и земно базиране (за някои ВКС – и средства с морско и въздушно базиране), предназначени за решаване на различни задачи [5: 79].

В зависимост от предназначението и вида на военните действия ВКС се подразделят на три основни вида:

− за осигуряване на военни действия;
− ударни (за космическо нападение);

– за противокосмическа отбрана.

Първите ВКС, въведени в експлоатация през 60-те години на XX век, са ВКС за осигуряване на военни действия. Те биват разузнавателни, навигационни, комуникационни, метеорологични, геодезични и спомагателни.

След първите разработки в края на 50-те и началото на 60-те години на XX век в САЩ и в СССР на ударни военно-космически системи през 70-те години започва тяхното интензивно развитие. Ударните ВКС са предназначени за водене на борба с различни космически обекти в космическото пространство и за въздействие по обекти в атмосферата и на земната (морската) повърхност. Имат компоненти с космическо и наземно базиране.

Военно-космическите системи за противокосмическа отбрана (ПКО) са предназначени за отразяване на нападение на противника в Космоса и от Космоса. Тези системи имат компоненти с наземно, морско, космическо и въздушно базиране и изпълняват три функции: предупреждение за ракетноядрен удар; контрол на космическото пространство; борба с космически летателни апарати (унищожаване или неутрализиране).

Така още през 60-те години на XX век става ясно, че господството в Космоса може да осигури превъзходство при провеждане на военни операции и води до надпревара във въоръжаването между САЩ и СССР.

В средата на 60-те години САЩ имат развърната система за прехващане и унищожаване на спътници с ракети, изстреляни от Земята. През 70-те години е приет на въоръжение противокосмически комплекс с въздушно базиране ASAT (Anti-Satellite). Използва се самолет F-15, който изстрелва ракета, клас „Въздух-Космос“ по космически обекти.

В САЩ се развиват организационно и структурите, които отговарят за използването на Космоса за военни цели. Първоначално структурите са в състава на Военновъздушните сили, но през 1985 г. е създадено Обединено космическо командване на въоръжените сили като основен орган за управление на космическите сили на страната.

В Съветския съюз в края на 60-те години на XX век е създаден противокосмически комплекс, наречен „ИС“ (изтребител на спътници), в който спътник прехваща, сближава се и на определено разстояние от друг космически летателен апарат се самовзривява. През 70-те години е създадена орбитална станция, предназначена да изпълнява както разузнавателни, така и ударни задачи от Космоса с изстрелване на ракети, клас „Космос-Космос“. В началото на 80-те години са приети на въоръжение противокосмически комплекс „Крона“, който използва изтребител МиГ-31 за изстрелване на ракети, клас „Въздух-Космос“, и лазерен комплекс с наземно базиране с възможности за откриване, прехващане и облъчване с лазерен лъч на космически летателни апарати с цел неутрализирането им.

Космическите средства в СССР през 80-те години на XX век са организирани във Войски за ракетно-космическа отбрана, включени в системата за противовъздушна отбрана на страната, но подчинени на Министерството на отбраната.

Използване на космическото пространство за военни цели в края на XX и началото на XXI век

В началото на 90-те години на XX век настъпва рязка промяна на военнополитическата обстановка в света, свързана с отпадане на идеологическото и военното противопоставяне между двете обществено-политически системи – западната и източната, в т.ч. и между САЩ и СССР. Съветският съюз се разпада, а Русия се превръща в регионална сила.

Разработките и използването на космически системи за военни цели обаче не спират. В тази дейност, освен САЩ и Русия, се включват активно и други държави.

Войната в Персийския залив през 1991 г. (операция „Пустинна буря“) се счита за първата космическа война. Многонационалните сили на антииракската коалиция развръщат космическа групировка от над 50 сателита, изпълняващи задачи по разузнаване, комуникации, оценка на резултатите от нанесените удари, за навигационно, топогеодезическо и метеорологично осигуряване. С това се постига огромно информационно превъзходство над противника.

В края на 90-те години настъпват редица промени във възгледите на военното ръководство на **САЩ** за използване на Космоса. Министерството на отбраната приема документа „Космически операции“, в който се посочва, че „безусловното военно превъзходство в Космоса е първостепенна задача на всяка военна кампания“. Военно-космическото превъзходство се предвижда да се завоюва чрез провеждане на противокосмически операции – настъпателни или отбранителни, с различни действия и оръжия, клас „Земя-Космос“, „Космос-Космос“ и „Космос-Земя“.

През 1999 г. е издадена директива на министъра на отбраната „Космическа политика на МО на САЩ“, в която Космосът е равнопоставен със сушата, морето и въздуха като среда за провеждане на военни операции. Въведено и формулирано е понятието „космическа мощ“ на държавата [5: 163].

Възгледите в САЩ за използване на космическото пространство за военни цели са развити в приетата през 2005 г. Космическа стратегия, която определя задачи, сред които са:

- активно осигуряване на свободен достъп на САЩ в космическото пространство за водене там на военна и друга дейност (в Космоса, от Космоса и чрез Космоса);
- защита и отбрана на космическите средства и системи на САЩ от всякакви въздействия с космически и други средства на противника;
- стратегическа противоракетна и други видове отбрана на САЩ с космически отбранителни средства;
- развръщане и бойно използване в Космоса и от Космоса на обикновени (неядрени) настъпателни и отбранителни космически средства (ядрените средства с некосмическо базиране се използват чрез Космоса);
- възпрепятстване на военния достъп в откритията Космос на вероятните противници, развръщане от тях в Космоса на военни настъпателни средства и използване на такива средства в Космоса и от Космоса срещу САЩ [4: 109 – 110].

Стратегиите за национална сигурност на САЩ също разглеждат проблемите за използване на Космоса. В тази от 2017 г. например е посочено, че Съединените щати трябва да поддържат своето лидерство и свобода на действие в Космоса [8: 31]. А в новата Стратегия за националната отбрана на САЩ от 2018 г. сред ключовите способности, които следва да се модернизират, са посочени и тези в космическото пространство като бойно пространство [9: 6]. В последвалата я нова Национална военна стратегия е представена идеята за съвместни обединени сили, които за постигане на военно превъзходство над конкурентите и неприятелите ще интегрират съвместните способности във всички сфери (домейни). Те трябва да воюват спокойно в Космоса или киберпространството така, както в другите три традиционни области (домейни) – на земята, на море или във въздуха.

В началото на 20-те години на XXI век Пентагонът планира различни програми и проекти за развитие на способностите си за водене на операции в Космоса и от Космоса.

Програмата „Blackjack“ предвижда извеждане на ниска околоземна орбита на гигантска групировка от малки спътници, позволяваща глобален обхват на всички военни операции на въоръжените сили. Счита се, че за Китай и Русия ще бъде по-трудно да унищожат подобна мрежа от малки и евтини спътници, създадени на основата на неособено скъпи комерсиални технологии, отколкото „малък брой скъпи, високотехнологични и уникални във военно отношение апарати“. Предвижда се тази групировка да решава задачи, като: постоянно глобално ранно предупреждение за изстрелване на ракети; индикация, предупреждение, прехващане и проследяване на ракетни заплахи; глобално ситуационно разузнаване в реално време; развитие на потенциала за сдържане; осигуряване на устойчива наземна инфраструктура за космическа поддръжка (наземни комуникационни станции и стартови ракетни площадки); постоянно глобално разузнаване на основата на системи с изкуствен интелект и др. [1].

Проектът „Авиационно-космическа система XS-1“ има за цел създаването на безпилотен космически апарат за многократно използване XS-1, чийто прототип е орбиталният апарат (космоплан) Х-37В, който осъществява полети в Космоса от 2006 г.

Програмата „Противоракетни лазери с космическо базиране“ предвижда създаване на космическа групировка от 20 военни лазерни платформи, разположени в орбити на отдалечение 1300 км от повърхността на планетата. Очаква се групировката да може в рамките на 2 – 5 секунди да унищожава бойните блокове на руските междуконтинентални балистични ракети, вкл. на РС-28 „Сармат“.

В рамките на проекта „Противоракетни системи с космическо базиране“ се предвижда в орбита да се извежда касетъчен модул с ракети прехващачи, насочени срещу ядрените ракети на противника, които ще бъдат изведени на балистична траектория в Космоса [1].

Друг проект предвижда изграждане на автономна орбитална космическа станция, което би станало почти 50 години след първата и единствена американска орбитална станция „Скайлаб“, изстреляна през 1974 г. и саморазрушила се през 1979 г.

Освен това в края на 2019 г. са създадени Космически сили на САЩ със свое командване. Те стават шести самостоятелен вид въоръжени сили, включен в състава на Министерството на ВВС. При обявяване на решението за създаването им президентът Тръмп казва, че „За Америка не е достатъчно просто да запазва присъствието си в Космоса. Ние трябва да доминираме в Космоса (...) Космосът е централен за националната сигурност и отбрана на Америка“ [6]. Следва издаване през 2020 г. от Пентагона на Стратегия за отбрана на Космоса и от Командването на Космическите сили на Доктрина за Космическите сили, озаглавена „Космическа мощ“.

Счита се, че в началото на 20-те години на XXI век от намиращите се на околоземна орбита над 1000 американски спътника особено важни са тези от серията КН-11. Това е секретната програма, изпълнявана от 1976 г., и се предполага, че спътниците от тази серия са най-съвършеното средство в арсенала на САЩ за оптическо космическо разузнаване, способни да различават обекти на Земята с размер до 15 см.

След края на Студената война космическите дейности с военно предназначение в **Русия** са сред важните държавни интереси.

В началото на 90-те години на XX век е приет на въоръжение модернизираният Противокосмически комплекс ИС-МУ, осигуряващ работа по маневриращи космическа цел и прехват на спътници на пресичащи се курсове. От началото на 20-те години на XXI век руски спътници, наречени „инспектори“, периодично се сближават с американски разузнавателни космически апарати.

В средата на второто десетилетие на XXI век е модернизиран и Противокосмическият комплекс „Крона“ с въздушно базиране на основата на изтребителя МиГ-

31. Малко по-късно изтребителят е въоръжен с по-съвършена противоспътникова ракета. По същото време са приети на въоръжение лазерни комплекси „Пересвет“, които имат задача да прикриват позициите на Ракетните войски със стратегическо предназначение чрез изваждане от строя на оптичните системи на разузнавателни спътници на противника.

Развиват се организационно и силите, изпълняващи задачи във и от космическото пространство. През 1992 г. са създадени първите Военно-космически сили към Министерството на отбраната на Руската федерация. През 1997 г. са създадени Ракетно-космически войски, в чийто състав са включени Ракетните войски със стратегическо предназначение, Военно-космическите сили и Войските за ракетно-космическа отбрана. През 2001 г. Ракетно-космическите войски са реорганизирани в Ракетни войски със стратегическо предназначение и Космически войски.

В началото на второто десетилетие на XXI век са създадени Войски за въздушно-космическа отбрана, които обединяват Космическите войски и структурите за противовъздушна и противоракетна отбрана. Силите и средствата за ракетно-космическа отбрана са организирани в три системи: за предупреждение за ракетно нападение, за противоракетна отбрана и за контрол на космическото пространство. През 2015 г. е извършена последната засега реорганизация чрез обединяване на Военновъздушните сили и Войските за въздушно-космическа отбрана във Въздушно-космически сили на Русия.

Дългосрочната руска политика в Космоса е регламентирана през 2013 г. в документа „Основни положения на Основите на държавната политика на Руската федерация в областта на космическата дейност в периода до 2030 г. и по-нататъшна перспектива“, утвърден от президента на Русия. В документа е посочено, че за реализиране на руските държавни интереси трябва да се осигури „поддържане на статута на Русия като една от водещите космически държави“, а като принцип на държавната политика в областта на космическата дейност е определена „защита на държавните интереси на Руската федерация в областта на космическата дейност с всички достъпни в рамките на международното право мерки и средства, включително признатото от устава на ООН право на самоотбрана“ [3].

От началото на XXI век се увеличават и амбициите на **Китай** в Космоса. Те са представени в документ на Държавния съвет през 2006 г. Планирано е създаване на няколко системи: за наблюдение на Земята, за дистанционни изследвания, спътникова навигация и за спътникови комуникации. В разработената програма за пилотируеми полети е предвидено извеждане на тайконавти (космонавти) на дълговременно функционираща в Космоса орбитална станция. Всички тези дейности имат и военно предназначение.

През 2007 г. Китай извършва успешен експеримент, при който с балистична ракета „Земя-Космос“ със среден обсег е извършен прехват и унищожаване на снет от експлоатация китайски метеорологичен спътник, изведен в орбита преди години. Спътникът е бил поразен на отдалечение около 865 км от Земята [5: 187]. След това Китай редовно извършва изпитания на такива ракети, наречени „убийци на спътници“.

През 2019 г. са извършени успешни изстрелвания на ракета носител от мобилна пускова установка, създадена на базата на пускови установки на междуконтинентални балистични ракети, както и от морски платформи. С това се разширяват китайските способности за атакуване и унищожаване на противникови сателити.

Изпълнява се и програмата за пилотирани полети в Космоса. През 2020 г. е извършен успешен полет на новата голяма китайска ракета носител „Long March-5B“, която е извела на предвидената орбита експериментален пилотируем космически кораб без екипаж и изпитателен космически апарат (капсула) за връщане на товари на

Земята. След няколко дни капсулата е кацнала успешно на територията на Китай [2]. С този полет започва изграждане и експлоатация на постоянна пилотирана космическа станция.

По оценки на експерти от 2018 до 2020 г. бюджетът за космически изследвания на Китай отстъпва само на този на САЩ, но по брой изстреляни ракети той е водеща държава в света [7].

С развитието на способностите си за провеждане на операции в Космоса, от Космоса и чрез Космоса с изграждане както на ударни военно-космически системи, така и на такива за противокосмическа отбрана, заедно с реализирането и на другите си космически програми Китай все повече се утвърждава като конкурентна на другите световни космически сили.

Технологиите за използване на Космоса за военни цели се развиват и в други държави.

През 2019 г. **Индия** осъществява успешно изпитание на противоспътниковата си система „A-SAT“, при което с ракета, изстреляна от Земята, успешно е унищожен друг индийски сателит. С това страната става четвъртата с противосателитна система след САЩ, Русия и Китай. **Франция** също развива свои космически програми. От началото на XXI век страната създава и използва за решаване на различни задачи както военни сателити, така и спътници с двойно предназначение.

НАТО също оценява значението на Космоса. В продължение на десетилетия Алиансът изпълнява своя програма за спътникови комуникации (SATCOM). През 2019 г. Космосът е обявен за „нова оперативна област (домейн) за провеждане на операции от Пакта, наред със сушата, морското, въздушното и киберпространството. Същата година НАТО приема своята първа космическа стратегия.

Заключение

Първоначално изкуствените спътници на Земята, известни още като „сателити“, се използват за наблюдение и разузнаване на наземни обекти. Постепенно военното им предназначение се разширява – за комуникации, навигация, метеорологични цели, картография, предаване на данни, прехващане на комуникации и др.

С развитието на технологиите се създават оръжия на нови физически принципи за унищожаване или неутрализиране на военни космически летателни апарати с различно базиране.

Така, едновременно с това, че днес космическите технологии имат все по-широко гражданско приложение и все по-голямо значение за човечеството, е безспорно, че Космосът се е превърнал в потенциално бойно пространство.

Литература

1. **Димитров,** Б. Милитаризацията на Космоса като елемент от геостратегията на САЩ. – В: *Геополитика,* бр. 3, 2020.
2. **Китайска** революционна ракета носител се приземи успешно. – В: *Nova.bg,* 8.05.2020 г. [достъпен 28.03.2024]. *https://nova.bg/.*
3. **Основные** положения Основ государственной политики Российской Федерации в области космической деятельности на период до 2030 года и дальнейшую перспективу, утверждены Президентом Российской Федерации от 19 апреля 2013 г. № Пр-906.
4. **Остапенко,** О. Н., С. В. Баушев, И. В. Морозов. Информационно-космическое обеспечение группировок войск (сил) ВС РФ. Учебно-научное пособие. Санкт-Петербург: Любавич, 2012.
5. **Пенев,** П. Космос и сигурност. Велико Търново: Витал, 2014.
6. **САЩ** създадоха космически военни сили. – В: *economic.bg,* 21.12.2019 г. [достъпен 18.03.2025]. *https://www.economic.bg/.*

7. **Стрекопытов,** В. Отношения с космически мащаб. Русия и Китай ще строят база на Луната. – В: *РИА* Новости, 22.03.2021 г. [онлайн]. [достъпен 29.03.2021]. *https://ria.ru/л*
8. **National** Security Strategy of the United States of America, December 2017. The White House, December 2017. [online]. *https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.*
9. **Summary** of National Defense Strategy of the United States of America – Sharpening the American Military's Competitive Edge, January 2018. Department of Defense, January 2018. [online]. *https://media.defense.gov/2020/May/18/2002302061/-1/-1/1/2018-NATIONAL-DEFENSE-STRATEGY-SUMMARY.PDF.*

НЯКОИ НЕОБХОДИМИ АКТУАЛНИ ПОДХОДИ НА СЛУЖБИТЕ ЗА СИГУРНОСТ И ОБЩЕСТВЕН РЕД ПРИ ПРОТИВОДЕЙСТВИЕТО НА СЪВРЕМЕННИТЕ ЗАПЛАХИ

проф. д-р Иво Великов
Университет по библиотекознание и информационни технологии – София

SOME NECESSARY CURRENT APPROACHES OF SECURITY SERVICES IN COUNTERING MODERN THREATS

Prof. Ivo Velikov, PhD
University of Library Studies and Information Technologies – Sofia

Резюме: *Докладът е опит да разкрием, опишем и прогнозираме съществени тенденции в основните дейности на службите за сигурност и обществен ред, в частност – на органите по разузнаването и контраразузнаването в нашата страна. На основата на личен анализ, опита в служби за сигурност и научноизследователска дейност повече от 30 години се разкриват предизвикателствата и необходимите промени в няколко съществени направления и основни задачи, с подчертано внимание към средата за провеждане на агентура.*

Ключови думи: *разузнаване; контраразузнаване; служби за сигурност и обществен ред; агентурно-оперативна работа; кадрова политика в структурите за сигурност; асиметрични заплахи; разузнавателен анализ; разузнаване по открити източници; техническо разузнаване*

Abstract: *The report is an attempt to reveal, describe and forecast significant trends in the main activities of the security and public order services, in particular – of the intelligence and counterintelligence bodies in our country. Based on personal analysis, experience in security services and scientific research for more than 30 years, the challenges and necessary changes in several significant areas and main tasks are revealed, with emphasis on the environment for conducting intelligence-operational work.*

Key words: *intelligence; counterintelligence; security and public order services; agent-operational work; personnel policy in security structures; asymmetric threats; intelligence analysis; open source intelligence; technical intelligence*

Темата произтича както от опита ми в служба за сигурност, така и от множество квалификации и научни изследвания през последните години – собствени и на колеги. Подходите, за които ще стане дума в този доклад, са плод на много години осмисляне на основните дейности на службите в контекста на асиметричните заплахи и динамиката на развитие на обществото.

На първо място, промяната в типичните за службите агентурно-оперативни подходи. Промяната през последните години се дължи на множество и все по-комплексни фактори, които влияят на използването на сътрудническия апарат:

1) Все повече изчезват класическите разузнавачи и контраразузнавачи, които залагаха на интелект, широки познания и ерудиция, които бяха силни в комуникацията „очи в очи“ (tete-a-tete). Доколкото при тоталитарните държави армия, полиция и служби са силно подкрепяни от държавата организационно и материално, развива се науката по сигурността, ползват се редица привилегии, то във времената на демокрация най-интелигентните и ерудирани млади образовани хора не са държавни служители. Като цяло интелектуалният потенциал на кандидатите за службите за сигурност

и обществен ред намалява. Изводът е на основата на 25 години преподаване по специалности, свързани с държавната служба.

Намалява делът на научното познание в оперативните дейности и развитието на оперативната работа – институтът по компютърни технологии на МВР беше закрит преди повече от 15 години, институтът по криминалистика на МВР от 10 години не е „научноизследователски“ (тази дума изчезна от името на НИКК), финансирането му и материално-техническата база са толкова трагични, че през определени периоди не могат да бъдат провеждани някои видове експертизи, а на експерти от института – участници в съдебни процеси из цялата страна, не се плаща с години. Институтът за специална техника беше преместен от МВР в ДАТО и преди две години закрит като досаден придатък на Агенцията. Вероятно единствено Институтът по психология поддържа някакво ниво на научна активност, несравнимо, разбира се, с времената преди 20 – 30 години.

Основният извод е, че в съвременната оперативна работа не се вижда необходимото развитие, залага се на остарели техники и технологии от времето на съветската школа, не се познават новите тенденции в агентурно-оперативната работа на водещите държави [7]. Същият извод е направен от А. Михайлов, който посочва, че „съществува и необходимост от познаване на чуждестранни практики за работа с доброволни сътрудници, на използваната терминология, на начините за привличане на сътрудници, на основите за вербовка, отчетност и основанията за прекратяване на отношенията с такива лица – т.е. на опита на държави, където уредбата е разгърната и на вътрешноведомствено, и на законодателно ниво“ (напр. вж. „Работата с информатори в американски военни и цивилни агенции. Поуки за Република България“ [7]). Дали някой се е запознал с това отлично изследване, например в СВР – МО, ДАР или ДАНС, или с „Разследване на шпионство“ [4: 75 – 89]), или с публикуваните от същия автор изводи за процесуално-следствени действия при разследване на шпионство („Някои процесуално-следствени действия при разследване на шпионство – съвременна практика“ [8])? В посочената статия от А. Михайлов е изтъкнато, че „само чрез система от процесуални действия и правилното им провеждане може да се осигури постигането на целите на разследването“. Тоест споделя се и направеният от мен извод за използването на модерни оперативни методи, съчетани със система от процесуални действия с оглед на повишаване на ефективността на прилагането им в разкриването и разследването на противодържавни престъпления.

Още един проблем, свързан с науката в оперативната работа, е капсулирането на гилдията. Професионалистите в СС от публичния сектор не приемат изследване от вън, т.е. от лице, което не е било в техните редици. За съжаление, професионалистите от разузнавателни звена от големи корпорации също не приемат външни лица за авторитети [11; 13] и също „пазят“ ревниво занаята си. Тоест кръгът на лицата, които имат достъп до истинска информация, както и до резултатите от разузнаването най-общо като дейност (и в публичния, и в частния сектор), не са някакво значимо число, а съвсем малко от тях – броени единици, имат някакъв стремеж към изследователска дейност или общественополезни и общодостъпни изводи. Все още интересът на външни лица към тази дейност е ограничен и от изискването за достъп до класифицирана информация и принципа „необходимост да се знае“. Декласифицирането на информация е възможно, но под строгия поглед на комисии, които са от вътрешни лица и които в общия случай се стремят да запазят класифицираността на информацията. По тези причини, дори да има желаещи за научни изследвания, те обикновено не са допускани.

През първите години на моята преподавателска и научноизследователска дейност често си позволявах да пиша по проблеми, класифицирани с гриф за сигурност.

След няколко години вече беше ясно, че и най-добрият труд вероятно ще бъде прочетен от 5 – 10 лица с достъп до класифицирана информация при крайна необходимост (която може и да не дойде). Така творчеството по дълбоко професионални проблеми просто прекратих.

2) Духовните, културните и интелектуалните потребности и навици на съвременните млади хора изначално не предполагат те да имат успех в комуникирането си в ролята на агентуристи от службите на нашата страна. Все по-малко разговарят помежду си, слабо познават различни професии, трудно навлизат в нови колективи, не познават като цяло корпоративния речник, професионалния жаргон по специалността (или директно – в службите за сигурност и службите за обществен ред). Сред моите студенти имам непрекъснато случаи в паузата за почивка в залата да бъде гробна тишина и всички да пишат на телефоните си и да четат в тях, но... не комуникират помежду си (говорим за млади мъже и жени между 20 и 30 години, свободни от семейни ангажименти, изучаващи една и съща специалност, по някакъв свой си странен начин искат да работят тази работа без никаква представа за реалните характеристики и параметри, а... (б.а. – цитирам най-срещаното мнение – „защото така иска от малък/малка и за това си мечтае“). Няма рационален мотив, а по-скоро емоционален, за работа в такива сложни и непознати системи.

Познати са случаи на провали във вербовката и работата със сътрудническия апарат още преди десетилетия – поради слаба комуникативност, притеснение от страна на служителя, слаба подготовка за провеждане на срещи и т.н., но в момента психологическите и интелектуалните качества на младите хора изобщо не са подходящи за агентурна работа.

Не се познават никакви автори – не става дума за научно творчество, говорим за художествена литература, която в областта на разузнаването, контраразузнаването, полицейските дейности, криминалистиката, психологията, историята (все науки, които са изискуеми в работата на агентуриста от службите) има в изобилие, но въпреки декларираното желание за работа в подобна професия никой нищо не знае и не е прочел поради какъвто и да е интерес или случайност. Напълно споделям мнението, че професионален език може да се гради от ранна възраст, стига да се четат романите на Богомил Райнов, Андрей Гуляшки, Албер дьо Каре, както и всички публикации за Ким Филби, Рихард Зорге, Ели Коен и т.н. Интензивната и високоинтелектуална работа в службите просто не може да бъде изпълнена от такива хора, колкото и желание да имат. И тук има нужда от СОП – технологията е позната от полицейските структури на САЩ и Великобритания и беше въведена у нас през 2014 г. от министър Ц. Йовчев [3].

Основният извод от написаното до момента: агентурно-оперативната работа трябва да се развива към нови основни направления най-вече поради все по-голямата вероятност в службите за сигурност и обществен ред да попаднат неподготвени физически, психически и интелектуално оперативни работници, които нямат способности и капацитета да водят дейността по класическите познати подходи.

3) В условията на намаляване на потенциала на човешкия фактор за агентурна дейност е необходима по-тясна специализация на длъжностните лица – да бъдат използвани в по-тесен кръг от разузнавателни активности. Тоест служителите трябва да изградят качества и увереност в професионалната работа чрез участие в повече на брой сравнително еднотипни дейности и чак след повече от 6 – 7 години да започнат внимателно да разширяват кръга на своите оперативни възможности. Горните разсъждения следват от нашия опит в държавни и частни структури като експерт и ръководител, вкл. и като ментор на млади колеги, постъпващи направо от университета.

И тук отново бихме предложили повсеместно използване на стандартни оперативни процедури като лекарство срещу изначално ниското ниво на подготовка на

кандидатите за работа в сектор „Сигурност“. И не само на подготовка – изначалните представи за дейността на службите за сигурност и обществен ред са някакви нелепо романтични – оръжие, бойна подготовка, гонки с автомобили, криминалистика. Никой не предполага, че защитата на сигурността и обществен ред е доста бюрократична работа – най-вече от кабинет.

4) Разнообразието на съвременните, най-често асиметрични, заплахи, необходимостта от различна експертиза за тяхното противодействие не позволяват една или няколко служби за сигурност или обществен ред да получат приоритетно задачите по противодействие на всички асиметрични заплахи. Заплахи, като пролиферацията, несъстоялите се държави (или региони от държави, където държавата не е в състояние да упражнява властта си – темата е доста дълга, в България също има обезлюдени региони, където живеят много възрастни хора и няма нито един държавен служител – няма кмет, няма учители, няма поща, няма полицай и т.н., тогава къде е държавата напр. в едно погранично село с 10 – 15 жители на средна възраст 78 години), трансграничната престъпност, не са възможни дори за най-мощните държавности. Съвременните терористични, а и множество престъпни организации със своята мрежова структура [5: 237; 6: 58 – 85], при която отделните клетки са неизвестни, не се познават и не са свързани помежду си (не се знаят членовете и броят им), а ръководителят не е йерархичен, по-скоро е идеолог и вдъхновител (справка „ИДИЛ“ и „Ал Кайда“), не се поддават на традиционните подходи за противодействие на службите за сигурност и обществен ред.

За традиционни или симетрични заплахи за националната сигурност се считат тези, произтичащи от дадени политически или дипломатически деятелности. Логично би следвало това положение да се вземе под внимание от лидерите на една държава или международен съюз и да се състави анализ на евентуални бъдещи действия от страна на недоволната държава (или недоволен съюз). Известно е също, че както официално обявените военни действия, така и политиката се води чрез световнопризнати и използвани принципи и схващания. Този факт е ключов за характеристиката на симетричните заплахи – те са възможно предвидими, защото се развиват на основата на дадени исторически и политически традиции, породени от международната практика.

Нетрадиционните или асиметричните заплахи за сигурността са всички останали рискове и заплахи, използвани в съвременни условия и целящи уязвимите места на дадена система за защита на националната сигурност. „Асиметрична заплаха“ е вид заплаха, в която се съдържат неконвенционални, нетрадиционни, непознати и неочаквани за противника тактики, действия или средства, срещу които противникът не може да противодейства успешно. Асиметричната заплаха представлява мислене, организация и действие, различни от тези на противника, с цел да се увеличат собствените предимства и да се използват слабостите на противника“.

Асиметричната заплаха произлиза от термина „асиметрия“, който се използва за характеризиране на отношенията между несъпоставими по мощ и статут опоненти, при които по-слабият противник е в състояние да нанесе сериозни поражения и вреди и да наложи волята си над по-силния. При този вид заплаха се използват нетрадиционни, непознати, и най-вече неочаквани за противника методи и тактики, срещу които се въздейства трудно поради това, че доста често времето за откриване на дадена дейност срещу националната сигурност е дълго [2].

Поради този извод смятаме за правилно да предложим:

- Необходима е бърза, компетентна и експертна намеса в наказателноправните текстове за регламентиране на престъпленията вследствие на съвременните асиметрични заплахи – кибератаките, хакерството и др.

- Необходимо е търсене на широка експертиза – със своя ограничен щатен състав службите не могат да притежават компетенции по всички съвременни асиметрични заплахи, поради което е необходима външна експертиза, т.нар. „аутсорсинг“ на някои дейности, чрез наемане на външни експерти (по подобие на Adecco – популярна платформа за намиране на временна трудова заетост, която всеки ден намира работа на около 3 млн. лица по цял свят). Веднага съм задължен да отбележа, че мои колеги преподават почти безвъзмездно в службите за сигурност, вероятно е експерти да работят в полза на националната сигурност по подобен доброволен начин, единствено с морални награди или референции за тяхната експертиза от страна на службите, които просто да ги рекламират пред други работодатели.

- Необходима е програма за публично-частно партньорство в сектора за сигурност точно в контекста на противодействие на асиметричните заплахи – съвместни дейности, обучения, операции и мерки с участие на държавни структури, структури на местната власт, частни организации, НПО, и дори отделни личности, които да организират дружен отговор най-вече на кибератаки, кибертероризъм, хакерство, финансови измами чрез информационни технологии, финансиране на тероризма, пране на пари и т.н.

Асиметричните заплахи ще продължават да бъдат спътник на човечеството, при това динамиката на процесите се засилва и все повече техни разновидности ще се появяват и най-нормално през първите месеци и дори години няма да бъдат нито изследвани, нито описани. Това положение е толкова ясно, че всяко усилие в такива изследвания ще трябва да бъде адмирирано, и дори рисково и необосновано изводите и заключенията от такива изследвания да бъдат прилагани в практиката на споменатите по-горе партньори в борбата с асиметрията като заплаха.

5) Ролята и мястото на OSINT. Разузнаването по открити източници трябва да заеме много по-сериозна роля в разузнавателната дейност най-вече поради предпоставките за спад в качеството и количеството на информацията от агентурни източници. Впоследствие ще коментираме парадигмата на разузнаването, но тук просто ще отбележим, че почти всяка информация – между 95 и 98 % от необходимата и полезна информация, може да бъде намерена в открити (некласифицирани и незащитени) източници. Традиционната представа за разузнаване като пъзел всъщност е пъзел на прекалено многото информация и трудността е намирането на тази информация от огромното количество „информационен боклук“ в информационното пространство. Интернет и социалните мрежи в този случай са „необходимото зло“ – там е налична информацията от открити източници, но както често се споменава, възможността стотици, хиляди и дори стотици хиляди да коментират една новина, губи качеството на експертизата. В недалечното минало на социалистическата тоталитарна държава в медиите щяха да се появят само коментари на истински експерти и – подчертавам – на никой друг.

В интернет на практика всеки се изказва и така се губи експертизата. Сред стотици – главно емоционални, снобски, лаишки и направо глупави, статии и коментари изключително трудно се открива истината. В момента откриването на истината е задача на разузнаването по открити източници, но не от малко, а от многото информация. И това е основната черта на съвременната парадигма на разузнаването. Цензурата при социализма спомагаше да се правят само коментари от знаещи, от практици и учени (дори и да са политически оцветени в полза на тоталитарната държава). Всъщност пропагандата чрез медии е цензурирана абсолютно, но това позволява до нашата страна и аудитория да достигат само стойностни продукции – книги, музика, филми от Запада, като „Роки“, „Крамер срещу Крамер“, „Лени“, „Ах този джаз“, „Чочарка“, „Апокалипсис сега“, „1984“ на Оруел, „Залезът на Запада“ на Шпенглер, класиците в

рока и оперната музика и т.н. В момента достига неограничено всичко (със забележката, че се появиха цензорите „фактчекъри“, но това е политическо решение на повечето глобализаторски партии и правителства през последните 7 – 8 години).

Въпреки проблемите OSINT на практика е незаменим помощник на службите, просто трябва да бъдат наети съответните експерти, разследващи журналисти, НПО и т.н. да направят изследванията, които службите не са в състояние да направят и да коментират.

И отново, както предложихме по-горе, необходимо е стабилно публично-частно партньорство. И тук можем да посочим като пример „Йейлския доклад“ от средата на 60-те години в САЩ. Шърман Кент прави поправка на количеството и качеството на получаваната информация в ЦРУ, като, основавайки се на демократичността на американския печат, вдига прогнозируемия процент на информацията от открити източници на 95 (при това е живял в началото и в средата на Студената война, точно когато шпионството има непоклатими позиции). За да покаже правилността на своята хипотеза, Кент прави експеримент с петима професори от университета „Йейл“, като им поставя задачата да подготвят доклад относно състоянието на въоръжените сили на САЩ, в който предмет са части, не по-малки от ниво дивизия, мощта на флота и авиацията (с описание на корабите и самолетите), при това, като използват само открити източници на информация. Работата по доклада продължила три месеца. В края професорите изготвили доклад от няколкостотин страници и обобщена справка от 30 страници. Оценката на Кент била, че докладът в около 90 % отчита точно състоянието на въоръжените сили. По ирония на съдбата докладът незабавно е засекретен от ЦРУ и станал известен като „Йейлския доклад“ [12: B7].

6) Ролята и мястото на анализа да се променят. Друг проблем на разузнаването и контраразузнаването, свързан със съвременната парадигма, е целеполагането на СС в новите условия. Като изхождаме от горните общоизвестни заплахи, „фокусът“ на анализа се измества от малко на брой значими заплахи, многократно и добре описани, с потенциал да нанесат огромни поражения, към много на брой, по-малко значими като глобален потенциал, но и неизвестни като източници и последствия заплахи. С други думи заплахи с по-нисък потенциал (обратно на случай на евентуална военна и политическа победа на НАТО, която би променила тотално живота на 50 % от населението на света и значително на другата половина), но и по-малко изолирани (взаимнообвързани заплахи), по-малко специализирани (години наред основните заплахи са военнополитически, но вече има много други) и без отделна държавна институция, която да е предназначена за противодействие.

Заплахата от разузнаване на чужда държава се преодолява в значителна степен с развитие на собствени органи за външно и вътрешно разузнаване, но заплаха от екокатастрофа, промяна на климата, масова бежанска вълна и др. под. не могат да бъдат решени с усилията на една организация, дори и специално за целта създадена. Новите заплахи не произтичат еднакво или директно от конкретно явление или процес – в много случаи те са следствие от поредица явления и процеси, без непременно те да имат проявление във всеки регион или държава или да имат еднакви нива на проявление. Така целите на СС, освен многобройни, се превръщат и в неоднозначни, неоднородни, неопределени и неедновременни (съвсем малко трансформираме четирите „НЕ“ на проф. Семерджиев като характеристика на средата за сигурност). Така и възможностите за координация и взаимодействие – ключово понятие при коалиционната сигурност – са много стеснени. На второ място глобалният обхват на явленията и процесите ще се засилва и от човешката активност. Поради тази причина СС, и най вече аналитичните структури трябва да разбират тази динамика на обществените

процеси както никога до този момент. Информацията ще бъде основна стока и ценност на съвременното общество дотолкова, доколкото аналитичните структури ще съумеят да я обработят и съответно своевременно да предадат на вземащите решения органи, като се съобразяват точно с тази динамика. Дори разузнавателната общност на САЩ си дава сметка, че анализът на информацията следва да бъде правилно дистрибутиран между многото и мощни информационни структури, които въпреки това сами не могат да се справят с целия обем и поради това обработената аналитична информация трябва да бъде споделяна (и то доброволно) сред нуждаещите се колеги и структури. По този начин се отхвърля още една част от старата парадигма на разузнаването – секретността и мнителността към другите СС, вътрешното съревнование и противопоставяне с цел доказване на кадърност и качества пред държавните и политическите елити [9].

Още една важна (четвърта) промяна в парадигмата на разузнаването – СС трябва да се фокусират главно върху разкриването и превенцията на заплахите за сигурността. Много по-малко ще им бъде необходимо да реагират, когато заплахите вече са се превърнали в реални или кризата вече е в ход, поради характера на самите заплахи, които изброихме по-горе. Известните методи на разузнаването – агентурното проникване, беседите „на тъмно“, визуалното наблюдение и наблюдението с портативни или други технически средства, биха помогнали за разкриването на тайни по старата парадигма на разузнаването и при традиционните форми на война с цел своевременно откриване на подготовка и провеждане на мощни, най-вече военни операции. Но за граждански конфликти, тероризъм, биологични или екологични заплахи (озоновата дупка или растежа на Сахара) тези методи не са адекватни. При това положение се връщаме отново да пледираме за предупреждаването, мониторинга, прогнозирането на развитието на тези заплахи, където също виждаме ролята на разузнаването основно по разкриване, изследване, прогнозиране и превенция на заплахите. Как то е очевидно, никой от тези процеси няма директна или опосредствана връзка с шпионската работа.

7) Ролята и мястото на техническото разузнаване. Под „техническо разузнаване“ следва да се разбира вид организация на разузнавателната дейност, при която основна роля в придобиването и фиксирането на интересуващите разузнавателната служба данни изпълняват техническите средства, обособени в самостоятелни организационни системи. Техническото разузнаване позволява на разузнаването да открива стратегически военни (действащи и експериментални) и военнопромишлени обекти, да получава достатъчно точни (за вземането на политически и военни решения) данни за някои тактико-технически характеристики на създаваните оръжейни системи и военна техника, да води наблюдение върху хода на разработката и изпитването им без непосредствено проникване на територията на разузнаваната държава. Техническото разузнаване осигурява достоверна разузнавателна информация, чието огласяване (за политически цели) по правило не застрашава с ликвидиране източниците ѝ. Поради това тя е по-достъпна за практическо използване, отколкото сведенията и данните, придобивани по агентурен път. Техническото разузнаване дава възможност да се наблюдават големи пространства по всяко време на годината и денонощието [10].

Например интегрираните системи за контрол на въздушния трафик представляват подобен пример. Те обединяват огромна по обем информация за проследяване на полети, основана на разписания, заявки и предварителна информация, но в същото време имат готовност за множество промени във времето, които изискват гъвкаво пригаждане към обективната среда на дейността: 1) различни метеорологични промени могат да променят курсове и маршрути, височина на полета и т.н.; 2) различни природни явления – избухването на вулкана в Исландия, земетресения на летищата

по излитане и кацане, прелетът на птичите ята в посока север-юг и обратно също са фактори, с които е необходимо да се съобразяват; 3) различни социални събития в държавите – кризи с насилие, стачки на служители на авиационните компании или летищен персонал също трябва да бъдат съобразени; 4) множество фактори, свързани с промяната на индивидуалната обстановка на всяко летище, – засилена терористична заплаха или терористичен акт, промяна на наредбите за излитане и кацане, откриване на летище или нова писта и терминали и т.н. Така схемите за въздушен трафик се превръщат в постоянно изменяща се величина, като комбинират комплекс от фактически обстоятелства с динамични промени.

И тук идва вниманието към въздухоплаването на световната общественост, вкл. като задача за решаване от службите за сигурност и обществен ред.

Подобно е положението с ръководството на корабоплаването: за да влязат и напуснат пристанището без предпоставки за някакви произшествия, движението на кораби се контролира много преди собствените териториални води, а също и след напускането им. В САЩ при наличието на новото Министерство за сигурност на територията (DHS) започва контрол на кораби от около 1000 мили преди американския бряг или от пристанището. По програмата „Maritime Domain Awareness“ на 1000 мили вече е възможен контрол на борда на плавателния съд, така че далече преди брега да се контролират товарите, а също и да се предотвратят евентуални атаки. Друга важна програма е „Инициативата за защита на контейнери“ (US Container Security Initiative (CSI)), където стандартизираните контейнери, влизащи на американска територия, са подложени на предварителен скрийнинг още на предходното пристанище, преди да влезе в американското. Целта е да се предотврати използването им за транспортиране и контрабандиране на оръжие за масово поразяване, екипировка за терористични атаки или терористични клетки и др., както и да се повиши сигурността на търговските връзки и стоковите потоци [1].

Смятаме, че подобни способности са целта на всяко разузнаване – чрез технически средства да управлява не само собствените процеси, но и най-съществените сфери на човешката и държавната дейност. И това е дейност в полза на цялата държавна администрация и обществеността, не само на структурите на сектор „Сигурност.

Литература и източници

1. **Великов,** И. Кратка теория на разузнаването. София: Албатрос, 2017.
2. **Държавна** комисия по сигурността на информацията. Рискови фактори за интересите на Република България в областта на защитата на класифицираната информация. Сборник лекции, 2020.
3. **Заповед** № 8121з- 205/18.06.2014 г.
4. **Михайлов,** Антон. Разследване на шпионство. – В: *Научен* алманах на ВСУ „Черноризец Храбър“, кн. 3, 2003, с. 75 – 89.
5. **Михайлов,** Антон. Доктрина за противодействие на мрежи, представляващи заплаха. – В: *Сборник* с доклади от научната конференция „Сигурност и икономика“, ВУСИ, 2019, с. 237. ISBN 9780-619-7343-24-3.
6. **Михайлов,** Антон, Иво Великов. Анатомия на терористичната група. Студия в съавторство. – В: *Военен* журнал, 2020, бр. 1 – 2, с. 58 – 85. ISSN 0861-7392.
7. **Михайлов,** Антон. Работата с информатори в американските военни и цивилни агенции. Поуки за Република България. Монография. София: За буквите – О писменехь, 2022. ISBN 978-619-1855-23-0.
8. **Михайлов,** Антон. Някои процесуално-следствени действия при разследване на шпионство – съвременна практика. – В: *Сборник* с доклади от национална научна конференция с международно участие „Сигурност и отбрана“, 2023. София: За буквите – О писменехь, 2023. ISBN 978-619-185-593-3.

9. **Попов,** В. Трансформация на РО на САЩ в контекста на събитията от септември 2001 г. – В: *Сборник* „Разузнавателна защита на конституционния ред в демократичната държава“, ВСУ, 2001.
10. **Трифонов,** Т. и др. Теория на разузнаването. Част първа. София: Фондация „Национална и международна сигурност“, 2011.
11. **Masterman,** J. C. The Double-Cross System in the War of 1939-1945. London: Yale University Press, 1972.
12. **Sullivan,** Patricia, Roberta Wohlstetter. Military Intelligence Expert. Obituary. – In: *Washington* Post, 10 Jan 2007, p. B7.
13. **Winterbotham,** F. C. The Ultra Secret. London: Weidenfeld/Nicholson, 1974.

ПОЛИЦЕЙСКОТО РАЗУЗНАВАНЕ И АНАЛИЗ НА РИСКА В СИСТЕМАТА НА ГЛАВНА ДИРЕКЦИЯ „ГРАНИЧНА ПОЛИЦИЯ“: ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ

проф. д-р Ставри Фердов
Академия на МВР – София

POLICE INTELLIGENCE AND RISK ANALYSIS IN THE BORDER POLICE DIRECTORATE GENERAL: CHALLENGES AND PROSPECTS

Prof. Stavri Ferdov, PhD
Academy of the Ministry of Interior – Sofia

Резюме: *Научният доклад е насочен към изследване на мястото и ролята на полицейското разузнаване (оперативно-издирвателната дейност (ОИД) в процеса на анализ на риска в системата на Главна дирекция „Гранична полиция“ в Министерството на вътрешните работи на Република България. Акцентира се както на сегашното състояние, така и на предизвикателствата и перспективите пред звената ОИД след влизането на България в Шенгенското пространство. Предложени са подходи за повишаване на приноса на ОИД на тактическо равнище.*

Ключови думи: *полицейско разузнаване; анализ на риска; Главна дирекция „Гранична полиция“*

Abstract: *The scientific report is focused on the study of the place and role of police intelligence (operational intelligence – OID) in the process of risk analysis in the system of the General Directorate of Border Police in the Ministry of Interior of the Republic of Bulgaria. It focuses on the current situation as well as the challenges and prospects for police intelligence units after Bulgaria's accession to the Schengen area. Approaches to enhance the contribution of the OID at tactical level are proposed.*

Key words: *police intelligence; risk analysis; Border Police Directorate General*

Увод

Средата за сигурност в света и региона е в етап на сериозна турбуленция. Водените войни до нашите граници и противоборството между Великите сили налагат своята императивна геополитическата рамка. В драматичната историческа линия на българската държава осланянето на Великите сили за решаване на национални задачи е водило до национални катастрофи.

Ние сме членове на НАТО, ЕС, влязохме в Шенген, предстои еврозона. Всичко това ни задължава да се държим като лоялни и надеждни партньори. В същото време именно актуалната геополитическа и геостратегическа рамка предполагат консолидация на наличния национален капацитет за отговор на външните и вътрешните заплахи и свързаните с тях рискове с цел защита на българските национални интереси.

Предметът на този научен доклад е мястото и ролята на полицейското разузнаване в процеса на анализ на риска в системата на ГДГП.

Роля на полицейското разузнаване и анализът на риска в системата на ГДГП

Системата на Главна дирекция „Гранична полиция“ е важна структура в състава на националните сили за контрол на границите на РБ и справяне със заплахи, като

нелегална имиграция, трафик на хора и наркотици, тероризъм, борба с контрабандата и останалите форми на трансграничната престъпност.

Полицейското разузнаване (оперативно-издирвателната дейност) в ГДГП е дейността, която е „очите и ушите“ за справяне с тези заплахи. Тя е призвана да минимизира или в добрия случай да премахва неопределеността в оперативната обстановка на границата. В конкретния случай за ГДГП обстановката носи в „снет вид“ признаците, белезите, факторите от далечната и близката среда за границата на РБ. Това е особеното за обстановката по границите. Или, ако се изразим с философски категории, тази обстановка е уникален микс между единично, особено и общо. Общото е далечната среда, особеното е регионалната, единичното е свързано с конкретиката на тактиката на действие (модус операнди) както на правонарушителите на границата, така и на нашата. За последната (нашата тактика) ОИД е необходимо да осигурява достатъчно надеждни данни за операциите и тактиката на граничните наряди като тактика на терен.

В този смисъл полицейското разузнаване в ГДГП по презумпция е водещо, лидиращо дейностите по анализа на рисковете в ГДГП. Това е така, защото всичко започва от придобиването на данните, тяхната обработка, систематизация и оценка, като база, на която ръководители на стратегическото, оперативното и тактическото равнище за ГДГП взимат решения, изразяващи се в отдаване на заповеди за граничния контрол. С други думи граничният контрол в ГДГП се провежда на основата на анализ на риска.

Всъщност именно дейността по обработка, систематизация и оценка на данните (разбирай анализ на риска) е начало на „бойната“ дейност. Поради тази причина повече от авторите предпочитат да говорят за това, че анализът на риска е част от разузнавателния процес (цикъл), а в подзаконови нормативни актове на ГДГП фигурира като първа точка от организацията на дейността [1: 83].

Анализът на риска е дейност, свързана с идентификация на заплахите и оценка на рисковете.

Още оттук ще кажем, че анализът на рисковете в системата на ГДГП се осъществява с водещата роля на полицейското разузнаване. Успехите на ОИД в ГДГП за последните години са осезаеми и много важни за системата. Само за миналата 2024 г. са неутрализирани няколко организирани престъпни групи, които продължават важни реализации, свързани с разпространението на наркотици и акцизни стоки.

В пирамидалната система на ГДГП се осъществява двупосочен информационен обмен: ГПУ/БГПК – РДГП – ГДГП. Информационният поток е по линия на секторите (групите) ЛКЦ, РКЦ и отдела НКЦ в ГДГП.

В системата анализът на риска е [3: 116] на основата на работни групи, в които са включени служители от всички направления и линии на дейност **с водещо място на ОИД.** На практика тези групи се ръководят в повечето случаи от оперативен работник в ГПУ, РДГП и зам.-директор по ОИД на ГДГП. Те носят отговорност пред директора (началника) за анализа и оценката на рисковете. **Такава е практиката и в другите гранични стражи – членки на ЕАГБО – ФРОНТЕКС (а нека да кажем и съобразявайки се с акцентите, направени в общия интегриран модел за анализ на риска за граничните служби на Европа – CIRAM): водещи са ОИД и координационните центрове, като на стратегическо и оперативно ниво там са позиционирани и секторът (групите, които не са щатно обособени на тактическо и оперативно ниво!) „Анализ и прогнози“.**

Капацитетът на системата за анализ на риска и полицейското разузнаване са „свързани съдове“. От 2023 г. се оценява и уязвимостта в изводна форма за всички новопоявили се заплахи.

Изключителна отговорност на ОИД е „Криминалният анализ“ в системата на ГДГП. Този анализ и използването на АИС „Криминален анализ“ е важна част от основите на противодействие на трансграничната престъпност, включително оценката за уязвимост.

Като цел е необходимо да се заложат повече служители, и то по линия на ОИД, с непосредствена отговорност по информационно-аналитичното осигуряване на анализа на риска, особено на оперативно и тактическо равнище. Още повече че тази задача се поставя за втора година в националния план след действащата Стратегия за ИГУ от 2020 – 2025 г. Осигуряването на щатни бройки за тези управленски равнища стои от много години, но сега при положение, че се осигуряват значителен брой щатове за системата на ГДГП, това е наложително. Понастоящем положението е следното: в РДГП и ГПУ щатове по дейност анализ на риска липсват, а с вътрешна заповед на директора и началника функционално са определени служители, отговарящи за анализа на риска в тези структури. Необходимо е създаването на група на ниво РДГП и отделен служител (служители) на ниво ГПУ (БГПК). Съвсем друг е въпросът, че тези щатни единици няма да решат основния въпрос за анализа на риска в ГДГП – изнасянето му извън канцелариите и овладяването на необходимите знания, умения и компетенции от граничния полицай в наблюдението и проверките.

Позволявам си да развия това схващане за тактическото ниво – ГПУ (БГПК). Това е особено наложително след влизането на България в Шенген, като на вътрешните ни граници се разчита особено на прилагането на т.нар. „компенсиращи мерки“ и на акцентирането именно на анализа на риска. Този служител (служители) би могло да е (са) част от групата ОИД в ГПУ и от цялостния разузнавателен цикъл. Това ще позволи много по-гъвкаво и надеждно да се оползотворяват оперативно значимите данни (информация)за нуждите на граничния контрол. Би могло да се помисли този служител да се превърне в свързващо звено между криминалния анализ на групата ОИД и анализа на риска на тактическо равнище. Тук може да се включи и участие в подготовката на всички нови профили (които е добре да се актуализират на 10 – 15 дни според динамичността на обстановката) и цялостното разузнавателно покритие на граничния контрол (граничните проверки и граничното наблюдение). В момента би могло да се твърди, че това покритие е опосредствано, не е директно, не е органична част от „бойната дейност“ (граничния контрол) на терен. За профилите се разчита и на оперативното ниво (РДГП), и на междуведомствените центрове по антитероризъм и миграция, но „теренът“ е най-динамичното и най-важното.

Тук изникват и редица въпроси, които са допълнителни, но много важни. Статистиката на Националното бюро за контрол на специалните разузнавателни средства е категорична: най-малък дял за използване на СРС от службите на МВР за петгодишен период има системата на ГДГП. Това само по себе си е сигнален индикатор.

От няколко години, след промяна на Закона за МВР, ОИД на ГДГП има правомощия на територията на цялата страна, а за да се подпише искането за използване на СРС в досъдебната фаза от наказателно производство, се идва до София. Тази ситуация е абсурдна и затруднява работата. Това е огромно правно предизвикателство и за разрешаването му в близко бъдеще ще продължи борбата.

Анализ на риска и информационно взаимодействие с оперативно-издирвателната дейност

Вътрешни информационни потоци

Всички направления и линии на дейност предоставят необходимата информация за анализ на риска. Особеното в областта на полицейското разузнаване е спазването на принципа „необходимост да се знае“. Би могло да се желае повече за своевременното връщане на необходимата информация от горе надолу след обобщаването на информацията на върха и формирането на ситуационни картини по граници.

Външни потоци и информационно взаимодействие

В настоящата ситуация според мен трябва да се върви изцяло към много близки форми на ползване на външни за системата информационни източници.

ГДГП ползва цялата информация от анализите на ЕАГБО (Фронтекс).

Идеята на Европейската стратегия за гранично управление е близкото ползване на информационен обмен между всички външни (извън страната) и вътре в страната, но извън ГДГП източници.

От външните за страната са важни откритите източници на ИНТЕРПОЛ, ЕВРОПОЛ, EASO, EULISA, МОМ, всички международни организации по антитероризъм, политологически и социологически сайтове в социални мрежи и „стари медии“ за комуникация.

Това информационно взаимодействие е важно за анализа на риска на ГДГП, за да не вървим в повечето случаи след събитията, само да ги регистрираме и да се опитваме конюнктурно и несистемно да им противодействаме.

Всичко това обаче е в „градината“ на разузнаването, респективно на полицейското разузнаване, респективно на ОИД на ГДГП. Това са хората, които трябва да ръководят анализа на риска на ГДГП. Всичко друго е регистраторство, констатиращо без формиращ ефект и „задружно участие в хора на учудените“ от събитията, които ни връхлитат. Всъщност това е основата на проактивния подход – само така могат анализите ни да завършват с вероятност за верни прогнози за границите на РБ.

От вътрешните за страната (но външни за ГДГП) са критично важни източници, като НРС, ДАНС, МВрРБ, МО, ДАБ, Агенция „Митници“, ГДНП, ГДБОП, ГДЖСОБТ, областни управители. Всички съвместни форми на анализ на риска (даже и „залинели“ през последните години) е необходимо да се възобновят и интензифицират.

В областта на **противодействието на престъпността през държавната граница настоящите предизвикателства продължават да са свързани с извеждането на рискови профили на лица, превозни средства и маршрути.** Ползват се рисковите профили с конкретни индикатори на ЕС (разработени от ЕВРОПОЛ и ЕАГБО) за чуждестранните бойци и лица, съпричастни към терористични групировки.

Моето разбиране е, че подготовката на постоянно възникващите нови рискови профили на тактическо ниво се нуждае от още по-активно информационно взаимодействие с ОИД. Нещо повече, рисковите профили трябва да се предлагат и подготвят от ОИД на тактическо ниво.

Последните години са силно доказателство за необходимостта от нова, още по-силна и ефективна роля на полицейското разузнаване на ГДГП в анализа на рисковете в граничната сигурност. Ще дам пример с каналджийството. Каналджийството и неговото противодействие не са нов елемент, но са особен акцент. За 2024 г. е установен значителен брой каналджии на българо-турската държавна граница. Именно

като действащо на територията на цялата страна полицейското разузнаване на ГДГП води, отговаря, лидира процеса на анализ на риска в граничната сигурност.

Бъдещи подходи вместо заключение

1. Осигуряване на нови щатни бройки за оперативно-издирвателната дейност и анализ на риска, и то най-вече за оперативното и тактическото ниво в системата на ГДГП. Моето мнение е, че горното е особено належащо за тактическото ниво и това е една от реалните мерки за постигане на още по-добри резултати в граничния контрол след влизане в Шенген.

2. Още по-голям акцент на подбора и обучението на анализаторите.

Подготовка на анализаторите

В Стратегията 2026 – 2030 г. за ИГУ е необходимо да се отдели място и на подготовката на анализаторите на ГДГП. Всеки от тях трябва добре да познава дейността и границата, за да анализира. Те непременно трябва да са минали през групите за охрана на границата или да имат стаж в групите ОИД. Недопустимо е служители, които не отговарят на тези изисквания и на специфичните аналитични способности, да заемат високи длъжности по пирамидата на ГДГП. Така се формализира и принизява процесът, обезсмисля се неговата полезност като първа фаза на управленското решение в ГДГП. Аргументацията на всичко това става още по-убедителна, ако желаем в бъдеще по-силна обектова специализация на анализаторите по отделните линии на дейност.

Подготовка на групите за управление на риска в ГДГП, РДГП и ГПУ/БГПК

Всички служители от групите в ГДГП, РДГП и ГПУ/БГПК е необходимо да минат курс за актуализиране на професионалната квалификация в АМВР „Анализ на риска в ГДГП“. Част от този курс е тактическият криминален анализ за оперативните работници. Там те придобиват знания, умения и компетентности в съответствие с общия интегриран модел на анализ на риска на ЕАГБО (Фронтекс) за идентификация, оценка и контрол на рисковете в ГДГП и криминалния анализ по стандартите на I-2 (Analyst Notebook).

Статията в никакъв случай не претендира за изчерпателност, много от същинските проблеми са избегнати, защото представляват чувствителна информация. Полето на дейност на ОИД е много обширно и важно за системата. Самите служители са натоварени с огромни отговорности, за което им дължим уважение и благодарности. Затова си мисля, че и в тези научни занимания понастоящем е добре да преобладава позитивният дух. Възприемам споделените подходи само като скромна част от пътищата за постигане на организационно усъвършенстване.

Литература

1. **Инструкция** № 8121з-1244 от 14.10.2015 г. за наблюдението на държавната граница на Република България, специфичната охранителна дейност за участие в мерките за постигане на летищна сигурност в обществените зони и периметъра на летищата и прилагане на компенсиращи мерки. – В: *ДВ,* бр. 83, 27.10.2015 г.
2. **Национална** стратегия за интегрирано гранично управление в РБ 2020 – 2025. Решение на МС 792, 30.10.2020 г. [онлайн]. *https://pris.government.bg/document/0320f0273e71316963db2598edfd1689.*
3. **Фердов,** С. Анализ и оценка на риска в контрола на държавната граница на Република България. София: Академия на МВР, 2012.

ИЗГРАЖДАНЕ И ПРИЛОЖЕНИЕ НА ПСИХОЛОГИЧЕСКАТА ТИПОЛОГИЯ НА ПОЛИЦЕЙСКИТЕ ИНФОРМАТОРИ

доц. д-р Емил Маджаров
Академия на МВР – София
д-р Йоанна Андонова-Цветанова
Институт по психология на МВР, Психологическа лаборатория – Благоевград
Камен Радев
ОДМВР – Пазарджик

CONSTRUCTION AND APPLICATION OF THE PSYCHOLOGICAL TYPOLOGY OF POLICE INFORMANTS

Assoc. Prof. Emil Madzharov, PhD
Academy of the Ministry of Internal Affairs – Sofia
Yoanna Andonova-Tsvetanova, PhD
Institute of Psychology of the Ministry of Internal Affairs, Psychological Laboratory – Blagoevgrad
Kamen Radev
Regional Directorate of Internal Affairs – Pazardzhik

Резюме: *Актуалността на настоящото теоретично изследване се задава от значимостта на психологическите типологии на полицейските информатори за тяхното вербуване, мотивиране и супервизиране в процеса на дейността им по разкриване и превенция на различни криминални деяния. Теоретичният анализ включва интерпретация на проблемите, възникващи при създаването и използването на психологическите типологии на информаторите в оперативната полицейска практика и вариантите за конструктивното им преодоляване.*

Ключови думи: *информатори; правонарушения; оперативни работници; личностни черти; мотивация; поведение*

Abstract: *The relevance of this theoretical study is determined by the importance of the psychological typologies of police informants for their recruitment, motivation and supervision in the process of their activities in the detection and prevention of various criminal acts. The theoretical analysis includes an interpretation of the problems arising in the creation and use of psychological typologies of informants in operational police practice and the options for constructively overcoming them.*

Key words: *informants; offenses; operatives; personality traits; motivation; behavior*

Актуалност на проблема

Актуалността на темата се определя от функционалния принос на психологическата типология на полицейските информатори за оперативните полицейски дейности по разкриването, пресичането и превенцията на различни криминални престъпления.

Психологическият профил на информаторите може да помогне на полицейските служители по-прецизно да установят тяхната лоялност и да селектират по-подходящи лица за сътрудничество. Точната идентификация на мотивите на информаторите може да облекчи намирането сред тях на готовите да сътрудничат доброволно, както и установяването на онези, по отношение за които е необходимо да се прилага

принуда и натиск. Тази диференциация дава възможност да се определи действителната ангажираност на информаторите и по-акуратно да се прогнозират пределите на лоялността им.

Някои типове личности могат да сътрудничат успешно и в условията на повишен стрес и фрустрация. Очевидно, те могат да работят продуктивно като полицейски информатори в рискови ситуации и да изпълняват задачи, свързани и с по-дългосрочно натоварване. Предварителното фиксиране на тези личностни предразположения на базата на психологически типологии сериозно може да оптимизира вербуването, подготовката и използването на информаторите в полицейското разузнаване. Анализът на психологическите характеристики може да обезпечи фиксиране на рисковите фактори за сътрудничество с информатори, които представляват заплаха за провал на полицейските дейности, като лоялност към престъпни групировки и техните лидери.

С основание можем да твърдим, че усъвършенстването и използването на психологически типологии на полицейските информатори е актуална изследователска дейност. От нейното успешно реализиране в значителна степен ще зависи ефективното управление на информационните ресурси за обезпечаване на обществения ред.

Теоретични основания

Полицейските информатори се типологизират с помощта на съответните критерии и въз основа на тях са определят различни обобщени техни персонажи, характеризиращи се с присъщата им разузнавателна функционалност, поведенчески и личностни качества [7; 1; 2].

Мотивация на отделните категории информатори предоставя възможност да се формира отделна тяхна типология. В нея се обособяват следните типажи:

**Информатори, сътрудничещи на полицията заради финансово възнаграждение. Това са личности с меркантилно-прагматични нагласи, оползотворяващи всеки източник на доход, или лица, стабилизиращи и повишаващи самооценката си чрез своите контакти с полицията.

**Сътрудници, осигуряващи информация заради устойчиво намерение за реализиране на възмездие по определен начин или обезпечаващи защита на близки и значими за тях хора, оказали се в трудно положение. Визираната група информатори могат да са много последователни в своето партниране с полицията, да проявяват решителност, да са пристрастни и тенденциозни при предоставянето на оперативна информация.

**Информатори, споделящи информация с полицията поради своите идеологически убеждения и цели [11]. Те възприемат подобен ангажимент като свое задължение, произтичащо от техните ценности. Този тип информатори преодоляват различни трудности, не икономисват енергията си и дългосрочно осъществяват полезните си контакти с полицейските служители, без да изпитват нужда от стимулиране.

Типологиите на информатори се структурират според степента на участието им в конкретна криминална дейност [9; 3; 10; 5]. Активните информатори са включени в извършването на престъпления и паралелно сътрудничат на полицията, тъй като се стремят към редуциране на неизбежното си наказание или се опитват да си осигурят други преференции. Те се отличават с повишен прагматизъм, голяма пластичност, двойственост и безпардонност и се опитват да си осигурят максимална полза в конкретната ситуация и да се предпазят от негативни последствия. Те внимателно селектират ценната информация, маскират деликатни нейни аспекти и за полицията и

престъпниците имат съответните варианти, които пускат в действие в зависимост от развитието на обстановката.

Пасивните информатори, предоставящи информация на полицията, не участват интензивно в криминална дейност, а понякога, във връзка с определено стечение на обстоятелствата, са в ролята на свидетели или извънгрупови наблюдатели. Качеството на тяхната информация за нуждите на предварителното следствие се определя от особеностите на функционирането на тяхната памет и внимание, от характерната за тях стресоустойчивост и от лоялността им към полицейската институция или към отделни нейни служители.

В съответствие с вида на осигуряваната информация се формират и типологии на полицейските информатори. В тях е включен и персонажът на техническите информатори. Те предоставят техническа информация на полицията в качеството си на компютърни специалисти и на други видове експерти. Надеждността на предлаганите от тях данни се определя от експертната им компетентност, от ситуационната им нагласа за колаборация с оперативните работници и от лоялността им към полицейската институция.

Очевидците са свидетели на криминални деяния, предоставящи информация на полицията. Качеството на сведенията, получавани от тях, са функция на пола, възрастта, когнитивното им функциониране, тяхната мотивация за конструктивно партниране с полицията, симпатиите им към разпитващия ги оперативен работник, сензитивността им на стрес, степента на тяхната включеност в конкретната ситуация на извършеното правонарушение [4; 3; 9; 10; 11].

Информатори със специални познания са лица със специални познания или с достъп до съответния вид информация, от която се нуждае полицията. Това могат да бъдат вътрешни хора в престъпни групи и организации, които са информирани за широк кръг криминални активности, експерти по пране на пари, производство на наркотични вещества, трафиканти на културни ценности и на хора [6; 5; 8; 2]. Много от тях са нарцистични персони, със значителен егоцентризъм, елитарни атитюди, твърде завишена самооценка и устойчиви самооправдателни защити. Партнирането с полицията за тях е необходимост, за да гарантират своя интерес, да избегнат евентуалните санкции или да редуцират проблемите си с конкуренти. Затова то може да бъде определено като конюнктурно, меркантилно, а предоставената информация е необходимо да се проверява сериозно.

Явните информатори доброволно сътрудничат на полицията като свидетели на престъпления или хора, които докладват за подозрителни дейности [4; 12]. Те често се включват като сътрудници по програми за сигурност или членове на общности, стремящи се към по-голяма безопасност. В индивидуален план това са личности с положителни нагласи към публичните ценности и полицията, хора с развито чувство за отговорност, с педантичен характер, предразположени да приемат и отстояват значими обществени каузи, търсещи повече признание, уважение и самореализация.

Негласните информатори работят под прикритие и не разкриват своето сътрудничество с полицията. Те участват в престъпни групи или имат близки контакти с хора, които са обект на полицейски интерес [4; 12; 1]. Негласните информатори се използват за събиране на информация за сложни престъпни мрежи и за разкриване на престъпления, извършвани в затворен кръг. Въпреки различията помежду им явните и негласните полицейски информатори играят ключова роля в борбата с престъпността и поддържането на обществения ред. В мотивационен план между двата вида информатори могат да бъдат идентифицирани редица прилики. Те обхващат мотивите за самоизява, осигуряването на признание и одобрение, нагласите за доминация и оказване на влияние върху други хора.

Това са различните видове психологически типологии на полицейските информатори. Във всяка една от тях има и съответните поведенчески подтипове и личностни характеристики, които са детайлизирани. Това им позволява по-ефективно да получат приложение в практическата полицейска дейност при прогнозиране на активностите на потенциалните информатори и регулиране на поведението на действащите сътрудници.

Методология

Цел на настоящото изследване е анализът на проблемите, възникващи в процеса на създаване и практическо използване на психологическите типологии на информаторите.

Задачите на теоретичното изследване са диференцирани по следния начин:

1. Установяване на основните трудности, появяващи се в хода на изграждане на различните типологии.

2. Идентификация и интерпретация на причините, ограничаващи реалното използване на психологическите типологии на информаторите в оперативната дейност на полицията.

3. Фиксиране на основните възможности за по-оптимално прилагане на създадените психологически типологии на информаторите в практиката на оперативните работници.

Предмет на изследването са проблемите при структурирането и използването на психологическите типологии на информаторите в контекста на полицейската дейност.

Обект на изследването са психологическите типологии на полицейски информатори, които се оползотворяват в актуалната практика на оперативните служби на полицията.

Хипотезата на настоящото теоретично изследване съдържа твърдението, че по-широкото използване на психологическите типологии на информаторите в оперативната полицейска дейност поражда проблеми, изискващи по-задълбочена и перманентна концептуално-методическа рефлексия, за да се оптимизира тяхното практическо внедряване.

Анализ на проблемите и трудностите

Мотивацията на информаторите, които партнират с полицията, е много нееднозначна, сложна, противоречива и в голяма степен неосъзната. За тях са характерни меркантилизъм, суетност, отмъстителност, повишен егоцентризъм. Информаторите се стремят да облекчат положението си заради очакваните санкции или са мотивирани от нагласите си за упражняване на власт над други правонарушители. Мотивите на много информатори са своеобразен „…микс от асоциалност, инфантилизъм, авантюризъм и хедонистична ориентация. Те успешно се справят в сложна ситуация, изискваща изразено самообладание, овладяване на стресовите преживявания и мобилизация на когнитивните процеси. Умението им да регулират емоциите си и фрустрационната им устойчивост гарантират успешното функциониране на когнитивните им способности, бързата реакция във възникналата ситуация и интуитивния избор на правилното решение“ [6: 20]. Въпреки сложната, прагматично-меркантилна, егоцентрична, хедонистична и компенсаторна мотивация на значителна част от полицейските информатори те ефективно изпълняват възложените им оперативни задачи и обезпечават своевременно важна информация. Следователно работещите психологически

типологии на информаторите трябва да отчитат специфичността на тяхната мотивация и да се освободят от морални стигматизации.

Справянето с конфликтите от информаторите предполага наличие на умения за преодоляване на трудности и предизвикателства, владеене на прийоми и техники за минимизиране на емоционалния стрес, произтичащ от непосредствените ангажименти. При тях той е следствие от риска, който се появява от участието им в определени дейности и отношения. Информаторите, притежаващи сангвиничен тип темперамент, побързо преодоляват стресовите си пренатоварвания при увеличаване на проблемите в разузнавателната им работа [13]. Очевидно, уменията за справяне със стреса са задължителен елемент от всички психологически типологии на информаторите.

В множество публикации [11; 2] рискът се разглежда като привлекателната страна в дейността на информаторите. Разузнавателните активности и на полицейските информатори са предпоставка за интензивни адреналинови преживявания при тях, които им дават възможност да се справят с големи рискове и да редуцират стреса си. За тях те изпълняват ролята на специфична категория мотивация, която има приоритетна функция и измества в този план техните користно-меркантилни и хедонистични мотиви. Посоченият вид мотивация в най-голяма степен спомага за минимизиране на стреса и фрустрацията, които са неизменна част от условията за работата на полицейските информатори.

За гарантиране на надеждността на полицейските информатори голямо значение има строгото следване на конспиративните правила. Това изисква формирането у тях на адекватно ниво на самоконтрол, изграждането на изпълнителност, дисциплинираност и саморефлексивност. Те трябва да не предозират адреналиновите си преживявания, инициращи предприемането на прекомерни рискове, прецизно следва да оценяват възникващите опасности, да не се увличат от голяма радост, задоволство и възбуда, които могат да притъпят тяхната бдителност и критичност [13] и да доведат до бърз провал. Затова индикаторите и проявленията на самоконтрола задължително трябва да присъстват при създаването и практическото приложение на типологиите на полицейските информатори.

А. Адлер специално подчертава значението на „...неосъзнатия стремеж към власт и превъзходство, който на поведенческо ниво се проявява като суетност, ревност и завист. Хората, които изпитват силна потребност от харесване и външно валидизиране, но не успяват да задоволят суетността си, често обезценяват другите, проявяват към тях враждебност и остро критично отношение“ [8: 12]. Тези техни атитюди обясняват ангажирането им като информатори и са фундамент на типологията, диференцираща ги в съответствие с желанието им за превъзходство и неговите превъплъщения в суетност, ревност и завист към отделните категории хора от престъпните среди. Персоналните ни наблюдения върху криминално проявените лица показват, че така теоретично структурираната типология има своя интерпретационен потенциал за обяснение на поведението и мотивацията на определен сегмент от групата на информаторите. Нейните обяснителни възможности не следва да се генерализират, както често се прави от изследователи психолози или от някои практикуващи полицейски служители, стремящи се да намерят универсално обяснение на комплицирания феномен на информаторите.

„Честото агресивно поведение прикрива комплекса за малоценност на извършителя. Според психоаналитичната теория изтласкването на чувството за малоценност се изразява в нереалистичен или антисоциален стремеж за превъзходство, който мотивира прикрита или директна вербална или физическа агресия. Хората с комплекс за малоценност непрекъснато се опитват да го компенсират, като се борят за превъз-

ходство, понякога с всякакви средства и начини“ [8: 43]. Визираните личностни особености и тяхното компенсиране са присъщи и на голям брой полицейски информатори. Осигуряването на сведения за други правонарушители им позволява да изразят своята агресия, да демонстрират собственото си превъзходство, да повишат самоуважението си и да осъществят социални интеракции в желано и значимо за тях обкръжение. Посочените психологически тенденции, механизми и ефекти трябва да бъдат разположени в основата на актуалните типологии на полицейските информатори и да представят комплицираната динамика на психичното им функциониране в характерни ситуации на трудности и опасности. Така те ще се приближат до реалния живот и ще обезпечат на оперативните работници задълбочена и точна визия за техните информатори, улесняваща резултатните им интервенции в хода на тяхното вербуване, мотивиране и инструктиране в различни ситуации.

Една прецизно създадена психологическа типология на информаторите има комплексни измерения и представя голям комплект от взаимносвързани личностнопсихологически качества и характеристики. При това закономерно се появява и сериозен парадокс. Колкото по-обемна и отговаряща на постоянно усъвършенстващите се научни стандарти е психологическата типология на информаторите, толкова намалява нейната практическа приложимост в оперативната дейност. Ако следваме всички изисквания, произтичащи от мощно изградена психологическа типология на информаторите, можем да останем без хора, чрез които да осигуряваме оперативно важна информация. Следователно психологическата типология е основа за ориентация и прогнозиране, позволяваща ни да планираме и реализираме съответните компромиси при подбора, вербуването и мотивирането на информаторите. За да бъде приложима теоретично и изследователски построената типология на информаторите, е задължително тя да бъде емпирично верифицирана и да е релевантна на множество реални ограничения, възникващи на принципа „тук и сега“.

Ползваните типологии от оперативните работници при работата им с информатори могат да бъдат консултирани с експерт психолог, който е участвал в тяхното създаване и има опит в прилагането им. Разбира се, отначало диалогът между двете групи специалисти със собствен опит и виждания за информаторите няма да се развива гладко, но в с течение на времето най-вероятно ще се оптимизира, което ще е от значителна полза и за двете страни. Конспиративността в работата с информатори не трябва да бъде сериозна пречка за деловата колаборация между криминалния психолог и оперативния работник и да служи за маскиране на нежеланието за контакт и на тревожните опасения от загуба на контрол над собствената професионална територия. Нормално е и двете страни, включени в този тип диалог, да притежават подобни опасения, но само в хода на съвместната работа те ще бъдат редуцирани.

Заключение

Съвременните психологически типологии на полицейските информатори следва по-пълноценно да презентират сложното разнообразие на тяхната мотивация, която е своеобразен микс от прагматично-меркантилни, егоцентрично-нарцистични, хедонистични и компенсаторни мотиви. Справянето с възникналите конфликти, преодоляването на стреса, изработването на оптимален толеранс към рисковите натоварвания и спазването на конспиративните изисквания са базовите основания при изработването и използването на психологическите типологии на полицейските информатори.

Неосъзнатият стремеж към власт и превъзходство и компенсирането на малоценностните преживявания определят в значителна степен спецификата на мотивацията и изпълнението на оперативните задачи от полицейските информатори. Затова те трябва да присъстват в психологическите типологии.

Ефективно структурираната типология на полицейските информатори трябва да съответства на установения научен стандарт и да е верифицирана в текущата оперативна дейност на полицията. Нейното успешно практическо приложение е свързано с установяването на полезна функционална колаборация между оперативните работници и криминалните психолози.

Направените от нас обобщения за психологическите типологии на информаторите потвърждават основателността на лансираната от нас хипотеза. Ефективното им внедряване в полицейската работа е съпроводено с непрекъснатото им усъвършенстване на базата на осъществената концептуално-методическа рефлексия на появилите се проблеми.

Литература

1. **Асенов,** Б. Теория на разузнаването. София: Албатрос, 2005.
2. **Асенов,** Б. Теория на разузнаването и контраразузнаването. София: Труд, 2012.
3. **Кардашева,** А. Психологията в оперативно-разузнавателната дейност. Силистра: Ковачев, 2007.
4. **Кунчев,** Й. Криминалистика от А до Я. София: Сиела, 2013.
5. **Маджаров,** Е. Психологическо портретиране на правонарушителите. Част 1 и 2. София: Сиела, 2006.
6. **Маджаров,** Е., Й. Андонова-Цветанова, Й. Джавелков. Личностни черти и мотивация на двойния агент. – В: *Бюлетин* на Факултет „Полиция“, бр. 11, 2023, с. 18 – 31.
7. **Начев,** Й. Вербовка и агентура. София: Труд, 2014.
8. **Стойчев,** Н. Насилието. Психологически анализ на местопрестъплението. София: Труд, 2016.
9. **Симеонов,** Ст. История и теория на обществената сигурност. Варна: Черноризец Храбър, 2021.
10. **Трифонов,** Т., С. Славов. Теоретични проблеми на разузнаването. Първа част. София: Национална и международна сигурност, 2000.
11. **Трифонов,** Т., В. Христов. Теория и технология на контраразузнаването. София: Сигурност, 2010.
12. **Христов,** В. Противодействие на чуждото разузнаване. Част 1. Варна: Черноризец Храбър, 2012.
13. **Христова-Стоянова,** Л. Разузнаването като социална дейност. – В: *Сборник* с материали от научна конференция с международно участие, Бургас, Бургаски свободен университет, т. 2, 2013, с. 59 – 66.

ПСИХОЛОГИЧЕСКИ АСПЕКТИ НА РАБОТАТА НА ОПЕРАТИВНИТЕ РАБОТНИЦИ ОТ ПОЛИЦИЯТА С ИНФОРМАТОРИ

доц. д-р Емил Маджаров
Академия на МВР – София
д-р Йоанна Андонова-Цветанова
Институт по психология на МВР, Психологическа лаборатория – Благоевград
Камен Радев
ОДМВР – Пазарджик

PSYCHOLOGICAL ASPECTS OF POLICE OPERATIVES' WORK WITH INFORMANTS

Assoc. Prof. Emil Madzharov, PhD
Academy of the Ministry of Internal Affairs – Sofia
Yoanna Andonova-Tsvetanova, PhD
Institute of Psychology of the Ministry of Internal Affairs, Psychological Laboratory – Blagoevgrad
Kamen Radev
Regional Directorate of Internal Affairs – Pazardzhik

Резюме: *Актуалността на психологическите аспекти на темата е свързана с ролята на полицейските информатори при разкриването, пресичането и превенцията на правонарушенията. Настоящото емпирично изследване е насочено към установяване на нагласите, предпочитанията и прийомите за работа на оперативните работници с различни категории информатори и влиянието върху това взаимодействие на социалнодемографския профил на служителите. Обект на емпиричното изследване са оперативни работници, пряко работещи с информатори в своята професионална дейност. Емпиричната верификация на хипотезите осъществихме чрез специално подготвена за тях блицанкета.*

Ключови думи: *информатори; оперативни работници; нагласи; мотивация; социалнодемографски профил*

Abstract: *The relevance of the psychological aspects of the topic is related to the role of police informants in the detection, interception and prevention of crimes. The present empirical study is aimed at establishing the attitudes, preferences and methods of working with different categories of informants of operatives and the influence on this interaction of the socio-demographic profile of the employees. The object of the empirical study are operatives directly working with informants in their professional activity. We carried out the empirical verification of the hypotheses through a blitz survey specially prepared for them.*

Key words: *informants; operatives; attitudes; motivation; socio-demographic profile*

Актуалност на проблема

Успехът в работата с полицейските информатори в голяма степен зависи от уменията на оперативните работници бързо и точно да се ориентират в реалната им готовност за сътрудничество. Те трябва прецизно да преценяват и ефективно да развиват тяхната ангажираност с възложените им разузнавателни задачи, както и лоялността им. Съвременният оперативен работник, осъществяващ полицейско разузнаване, трябва да е в състояние да прогнозира рисковото поведение на информаторите

и тяхната стресоустойчивост, за да предприема адекватни интервенции за стабилизация на мотивацията и действията им в подобни условия.

Ефективната дейност на полицейските служители с информатори е перманентен процес на координация и контрол върху техните активности с цел избягване на пропуски, грешки и провали. Своевременното им преодоляване зависи от спецификата на представите, нагласите, предпочитанията и прийомите на работа на оперативните работници с информаторите. Затова техният по-задълбочен психологически анализ има актуално значение.

Теоретични основания

По начина на рекрутиране информаторите се диференцират на две обособени групи. В едната от тях влизат доброволните информатори, към които се отнасят лица, доброволно предоставящи информация на полицията [5; 1; 2]. Те могат да се включват в подобна форма на сътрудничество в качеството си на явни и секретни сътрудници заради желанието си за самоутвърждаване, доминация, упражняване на влияние, получаване на социален престиж. Изброените мотиви на информаторите за сътрудничество с полицията могат да са свързани с такива личностни черти, като повишен нарцисизъм, изразена екстравертност, макиавелизъм или малоценностен тип самооценка. Те могат да предизвикват агресивно-враждебните нагласи на оперативните работници, безсъзнателно да ги инициират да се държат дистанцирано, недоверчиво и подозрително, да се стараят по-усилено да контролират поведението им, постоянно да проверяват получаваната от тях информация и индикаторите за лоялността им. Същевременно визираната трупа информатори може да се отличава с добри оперативни възможности, поради което оперативният работник трябва да се опитва да им демонстрира приемане, загриженост и да поддържа мотивацията им за работа. В този смисъл той следва да ограничава своите нагласи и предпочитания, да маскира собствената си подозрителност и интензивно да прилага различни манипулативни прийоми за постигане на близост, доверие и готовност за съвместна работа.

Във втората обособена група според начина им на рекрутиране попадат контролираните информатори. Това са лица, които са под наблюдение или над тях полицията упражнява контрол най-често заради престъпни дейности, които са извършили [4; 2]. Те са личности с развиваща се криминална кариера, множество престъпни контакти, натрупан криминален опит. Отличават се с прагматизъм, меркантилизъм и добър самоконтрол в сложни ситуации, наситени със заплахи и рискове. Контролираните информатори успешно могат да влязат и в ролята на секретни информатори, защото са въздържани, могат да бъдат респектирани и в определена степен да сътрудничат с полицейските служители. Те са особено ценни заради своите контакти и добра информираност за криминалните дейности на различни други правонарушители. Парадоксалното е, че те могат да импонират на оперативните работници, тъй като умеят да бъдат изпълнителни и дисциплинирани, да спазват изискванията на конспирацията и да осигуряват ценна информация. Независимо от това бдителността към тях не трябва да се притъпява и внимателно трябва да се наблюдават тяхното поведение и мотивация в различни ситуации, тъй като те не са константни даденост.

Информаторите, предоставящи данни заради персонални мотиви, свързани с намерения за отмъщение или обезпечаване на защита на близки значими хора, попаднали в комплицирана ситуация, могат да са много последователни в своето сътрудничество с полицията, да проявяват готовност за включване в рискови начинания, при които получаването на разузнавателни данни е съпроводено с конкретни опасности. Трябва да се отчита обстоятелството, че те са много ожесточени, пристрастни и готови

да злепоставят правонарушителите, за които предоставят актуална и значима оперативна информация. Те могат да изпълняват ролята на явни и секретни сътрудници. Това налага специално да бъдат инструктирани и внимателно да се минимизира високата им враждебност, да се наблюдава актуалната им мотивация и внимателно да се селектират, проверяват и анализират осигурените от тях данни.

Активните информатори на високи обороти са включени в престъпна дейност и паралелно сътрудничат с полицията в качеството си и на секретни сътрудници, за да получат намаление на наказанието си или други ползи. Те проявяват значителна гъвкавост, двойственост и прагматичност и се опитват да си осигурят максимална полза от ситуациите [3], в които попадат, за да редуцират негативните последствия и дискомфортните за тях законови санкции или престъпни възмездия. Поради това активните информатори в повечето случаи специално подбират важната информация, маскират отделни нейни аспекти и за всеки от партньорите си (полицията или правонарушителите) представят режисирани варианти за депозиране или правят оригинални интерпретации според възникналата ситуация.

Представените категории информатори специфично взаимодействат с оперативните работници, имащи определен социалнодемографски профил, влияещ на техните представи, нагласи, предпочитания за този тип колаборация и на прийомите за нейното осъществяване.

Методология

Целта на емпиричното изследване е диагностициране на нагласите, представите, предпочитанията и прийомите на работа на оперативните работници с информатори и влиянието върху тях на социалнодемографския им профил.

Задачите на емпиричното изследване са:

1. Определяне на нагласите, предпочитанията и прийомите на оперативните работници в работата им с явни и секретни информатори.

2. Оценка на представите и нагласите на оперативните работници за качествата на информаторите и рисковете при взаимодействието с тях.

3. Установяване на нагласите на оперативните работници с различен стаж за работа със секретни информатори със съмнение за контакти с правонарушители.

4. Регистриране на визията на оперативните работници за ценните качества на информаторите и влиянието върху нея на техния пол и продължителността на стажа им на оперативна длъжност.

Предмет на емпиричното изследване са нагласите, предпочитанията, представите, прийомите на оперативните работници за работа с различни информатори и влиянието върху тях на социалнодемографския им профил.

Обект на емпиричното изследване са оперативни работници от две населени места в страната, непосредствено взаимодействащи си с явни и секретни сътрудници.

Хипотезите на емпиричното изследване са:

1. Допускаме, че оперативните работници са с нагласата да привличат информаторите с убеждение след серия срещи, използвайки различни прийоми за мотивирането им. Предполагаме, че те предпочитат да работят с явни доброволци сътрудници заради тяхната добронамереност, а към секретните информатори изпитват съмнение в лоялността им.

2. Допускаме, че оперативните работници, взаимодействащи си с информатори, се напрягат от дефицита на лоялност, но смятат, че е умерен рискът от едновременното им сътрудничество с полицията и правонарушителите. Предполагаме, че те

нямат единни предпочитания относно прийомите за мотивиране на информаторите и им възлагат задачи, съобразени с оперативната обстановка.

3. Допускаме, че оценката на оперативните работници за риска секретните информатори да сътрудничат на полицията и правонарушителите ще корелира позитивно с предпочитанията за работа с тях и с броя на привличанията им за сътрудничество и отрицателно ще корелира със стажа на служителите на оперативна длъжност.

4. Допускаме, че ценените качества на информаторите от оперативните работници отрицателно корелират с техния пол и със стажа им на оперативна длъжност в полицията.

Емпиричната проверка на формулираните хипотези реализирахме чрез конструирана от нас блицанкета. Тя се състоеше от въведение и 16 затворени въпроса. Закритите въпроси от блицанкетата се диференцираха на съдържателни и социалнодемографски. Съдържателните въпроси бяха общо десет и за всеки от тях бяха подготвени по четири отговора. Респондентът трябваше да избере само един от тях и да го маркира. В съдържателните въпроси се засягаха темите за типовете информатори и качествата им, тяхното привличане за сътрудничество и мотивация, съществуващите рискове в процеса на работа с тях.

Социалнодемографските въпроси на блицанкетата бяха шест и маркираха пола, възрастта, образователния ценз, стажа в МВР и стажа на оперативна длъжност на служителите. Избрахме блицанкетата като вариант на методика за провеждане на емпиричното изследване, тъй като тя бързо се попълваше от респондентите, които са ангажирани делови хора и не трябваше дълго да бъдат откъсвани от непосредствените им задължения. Формулировките на изследователските хипотези непосредствено кореспондираха със съдържанието на въпросите от блицанкетата, както и с подготвените за всеки въпрос варианти на отговор. Отделните въпроси бяха така структурирани, че да осигурят точно разбиране на представения вербален материал и да не активират съпротивите на анкетираните служители. Получените с помощта на блицанкетата емпирични резултати систематизирахме в отделна таблица и по отношение на тях извършихме статистическа обработка с непараметрични методи. Използвахме хиквадрат за извършването на честотен анализ на данните и коефициента за корелация на Спирман.

В изследването взеха участие 30 оперативни работници, взаимодействащи си с различни категории информатори.

Болшинството участници в анкетата (96 %) са от мъжки пол. Те са склонни към реалистични и прагматични оценки по отношение на информаторите и проявяват умерена критичност, подозрителност и резервираност към тях. Във възрастовия диапазон от 31 до 45 години попадат 70 % от респондентите. Това са служители в активния период на професионалната си кариера, натрупали житейски и служебен опит, с добро ниво на мотивация и развити компетентности за оперативна работа. Установихме, че 83 % от анкетираните служители имат висше образование „бакалавър“, което също ги подпомага в дейността им с представителите на криминалния контингент и със самите информатори.

Близо 70 % от взелите участие в анкетата респонденти са в системата на МВР от 11 до 15 години. Всички те имат опит в работата с криминалния контингент, общували са с информатори и бързо се ориентират в тяхната мотивация, чувства, настроения, предпочитания, ниво на лоялност, актуални проблеми.

Анализ на получените резултати

Според резултатите от *Таблица 1* 53 % от анкетираните оперативни работници често прилагат в своята дейност прийома на постепенно убеждаване и реализирането на серия срещи с бъдещите си информатори.

Констатирахме и статистически значима разлика между разглеждания прийом и другите прийоми за привличане на информатори за работа. Повечето оперативни работници реализират търпелива комуникация от убеждаващ тип за привличане на информатори за сътрудничество и разчитат така да постигнат позитивен резултат.

Резултатите от Въпрос № 2 на блицанкетата сочат, че сред оперативните работници има неоднозначни нагласи към използваните в дейността им с информаторите мотивационни прийоми. Част от тях разчитат на финансовите стимули, а други са убедени в значението на личната връзка с информатора или на неговите идейни убеждения за поддържането на неговата мотивация за работа. Мотивацията на хората е твърде специфична и индивидуална. Поради изтъкнатите причини и между фиксираните отговори на втори въпрос от блицанкетата не бяха установени статистически значими различия.

В данните от блицанкетата за Въпрос № 3 установяваме, че 57 % от участвалите в анкетата полицейски служители предпочитат да работят с явни доброволни сътрудници. Това се дължи на разбирането им, заявено също от 57 % от тях (Въпрос № 4 от блицанкетата), че те са добронамерени и добросъвестни. Според 67 % от полицейските служители най-важното качество, което трябва да има секретният информатор, е да бъде достатъчно лоялен (Въпрос № 5). Тези резултати са индикатор за сериозни съмнения от страна на оперативните работници в лоялността и добросъвестността на всички категории информатори, които в съвременната динамична и прагматична социална реалност твърде много демонстрират повишен конформизъм, нагласи за двойствено поведение, лицемерие, неискреност и манипулативност.

Оперативните работници са оценили в анкета мотивационните прийоми за работа с информатори, описани в специализираната литература, имащи разпространение в практиката. Всички коментирани до момента данни са представени в *Таблица 1.*

Потвърди се тезата за наличието на множество прийоми за мотивиране на информаторите. Тази тенденция има своите плюсове и минуси. Оперативните работници трябва гъвкаво да се адаптират към работата с криминалния контингент, но прекаленото разнообразие на мотивационни прийоми показва и недостатъчната ефективност на всеки от тях и отсъствието на професионални стандарти за прилагането им. Откроихме два подхода при възлагането на задачи на нови информатори. Единият е по-рисков и носи конюнктурни ползи. Другият предполага постепенно обучение на информатора, за да се разширят неговите разузнавателни и личностни умения и да се намалят рисковете от провал.

Данните от Въпрос № 16 от блицанкетата показват, че 77 % от служителите са със стаж на оперативна длъжност от 4 до 15 години. Между резултатите по показателя „Стаж“ на анкетираните оперативни работници има статистически значими разлики ($p=0,011$). Те не само са усвоили своята професионална роля, но и умеят да селектират информатори, бързо се ориентират в техните личностни особености и разузнавателен потенциал, знаят как да ги вербуват и мотивират за работа, да неутрализират техните колебания, манипулативни опити и опасения. Всички направени коментари потвърждават правомерността на тезата, че работата с по-малко на брой информатори може своевременно да осигури получаването на необходимата оперативна информация и да гарантира конспиративността и конфиденциалността на контактите.

Таблица 1. **Честотен анализ на отговорите от съдържателните въпроси в блицанкетата**

1. Според Вас как най-често са привличани информатори за работа?	№	2. Как са били мотивирани информаторите за работа по време на сътрудничеството с тях през годините?	№	3. С какви информатори предпочитате да работите?	№	4. Какви качества трябва да притежават явните информатори (очевидци на престъпление, свидетели, доброволни сътрудници)?	№	5. Какви качества трябва да притежава секретният информатор?	№
След еднократна беседа	7	На идейна основа	7	Явни – свидетели на криминално деяние	2	Наблюдателност	5	Добра информираност за действията на правонарушителите	3
С постепенно убеждаване и серия срещи	16	На базата на лична връзка	8	Явни – доброволни сътрудници	17	Услужливо работеща памет	3	Да владее конспиративните прийоми	3
Самопредлагане	1	Чрез използване на финансова зависимост	7	Негласни – секретни	11	Добросъвестност и добронамереност	17	Да бъде достатъчно лоялен	20
С помощта на други начини	6	Възникване на друг тип зависимост	8	Явни – свидетели на криминално деяние	2	Безпристрастност	5	Да не използва положението си за прикритие на друга престъпна дейност	4
$X^2_{(3)}$=15,600, p=,001		$X^2_{(3)}$=0,133, p=,988		$X^2_{(2)}$=11,400, p=,003		$X^2_{(3)}$=16,400, p=,001		$X^2_{(3)}$=27,867, p=,000	

6. Кои личностни особености на секретния информатор ценните в най-голяма степен?	№	7. Какъв е рискът секретни информатори да сътрудничат едновременно с полицията и правонарушителите?	№	8. Според Вас кои приёми за мотивиране на информатори, описани в специалната литература, получават по-широко разпространение в реалната практика?	№	9. Какви задачи следва да се поставят на негласните информатори след тяхното привличане?	№	10. Кои са основните проблеми в работата с явни и негласни информатори?	№
Комбинативност и изобретателност	3	Много висок	10	Финансовите стимули	8	Задачи, съобразени с оперативната обстановка	16	Тяхната лоялност	16
Лоялност	23	Висок	3	Принудата и заплахата	9	Задачи, съответстващи на възможностите на информатора	9	Поставяне в определена зависимост от оперативния работник	7
Готовност да рискува в трудна ситуация	3	Умерен	17	Патриотичните апели и внушения	11	Задачи по определен казус за получаване на конкретна информация	4	Изкривяване на информацията	4
Упоритост за достигане до краен резултат	1	Умерен	17	Стремежът за лично отмъщение	2	Задачи, свързани с разяснение и съответна легенда за придобиване на информация	1	Злоупотреба с доверието на оперативния работник	3
$X^2_{(3)}$=43,067, p=,000		$X^2_{(2)}$=9,800, p=,007		$X^2_{(3)}$=6,000, p=,112		$X^2_{(3)}$=17,200, p=,001		$X^2_{(3)}$=14,000, p=,003	

Данните от Въпрос № 7 на блицанкетата свидетелстват, че оперативните работници внимателно преценяват риска от деловата колаборация на информаторите както с тях, така и с правонарушителите. Тази им преценка положително кореспондира с техните нагласи за работа с конкретна категория информатори и с количеството на привлечените за сътрудничество лица. Тя обаче отрицателно корелира със стажа

на служителите на оперативна длъжност в полицията (данните са представени в *Таблица 2*). Налице е естествен стремеж на оперативните работници да не бъдат манипулирани от информаторите, което закономерно пресява и редуцира контактите с тях. Следва да подчертаем, че особеностите на оперативната дейност е такава, че рисковете от взаимодействието с информатори са характерни за нея. Много оперативни работници притежават по-толерантни нагласи към множеството рискове в дейността си с информаторите. Затова в определени моменти те са склонни да я интензифицират и да повишат броя на лицата, с които поддържат контакт.

Таблица 2. **Значими корелации по част от въпросите в блицанкетата**

		3. С какви информатори предпочитате да работите?	11. С колко информатори (явни, негласни) работите по разкриване на престъпления?	14. Вашето образование?	16. Стажът Ви на оперативна длъжност в МВР е?
7. Какъв е рискът секретни информатори да си сътрудничат едновременно с полицията и с правонарушителите?	Correlation Coefficient	,471**	,449*	,365*	-,411*
	Sig. (2-tailed)	,009	,013	,047	,024
	N	30	30	30	30

Натрупването на стаж в процеса на оперативна работа в полицията прави служителя по-предпазлив, примерен и дозиращ собствената си професионална активност, за да се редуцират поне част от евентуалните рискове. Тази нагласа към дейността с информаторите може да бъде разбрана *(Таблица 2).* Тя е следствие от противоречивата обществена ситуация и организационен контекст на полицейската структура. Посочената индивидуална нагласа не осигурява необходимата служебна ефективност. Затова по отношение на нея последователно следва да се интервенира с управленски средства, за да се стигне до определеното ѝ минимизиране.

Регистрирахме наличието на отрицателна корелация между представата на оперативните работници за съществените качества на информаторите, тяхната полова идентификация (r=-,362, p=0.049) и продължителността на стажа им на оперативна длъжност в полицията (r=-,374, p=0.042). Функционалните качества на информаторите, като комбинативност, упоритост, готовност за поемане на рискове, за опитния оперативен работник с по-дълъг стаж не са от първостепенна важност, тъй като той цени преди всичко лоялността им. Това ранжиране на оценките за ценните качества на информаторите от оперативни работници с продължителен стаж е резултат на натрупан отрицателен персонален опит от колаборация с тях, на преживяване на редица възникнали инциденти, трудности и проблеми. Трябва да посочим, че мъжете оперативни работници по-еднозначно, рационално и критично разглеждат качествата на информаторите и за тях лоялността има водещо значение. Обработеният емпиричен материал потвърждава основателността на твърдението, че представите на оперативните работници за ценните качества на информаторите отрицателно корелират с техния пол и със стажа им на оперативна длъжност в полицията.

Заключение

Оперативните работници вербуват информатори за работа с убеждаване чрез множество срещи, използвайки различни мотивационни прийоми. Те осъществяват контакта с бъдещите информатори постепенно, изграждайки доверителен контакт, и постепенно ги мотивират за извършването на съвместна дейност. Оперативните работници желаят да работят с явни доброволни сътрудници заради тяхната добросъвестност. Те са сериозно резервирани и подозрителни към секретните информатори. Дефицитът на лоялност на информаторите безпокои оперативните работници, но те се адаптират към риска от възможното тяхно паралелно сътрудничество с полицията и с правонарушителите.

Използването на множество прийоми за мотивирането на информаторите от оперативни работници има положителни и отрицателни нюанси. Оценката на риска от оперативните работници за двойното сътрудничество на информаторите с тях и с правонарушителите интензифицира нагласите им за по-активна работа и за разширяване на броя на лицата за сътрудничество. Днес рисковете от нелоялно и двойствено поведение на информаторите са значителни. Тази негативна тенденция може да се редуцира само чрез по-резултатна работа с тях, което означава ползване на повече информатори, по-ефективното им мотивиране, супервизиране, контролиране и подкрепяне в по-сложни ситуации, както и с внимателно селектиране на сведенията, постъпващи от тях. Съществуващите по-самосъхранителен тип нагласи сред оперативните работници при работата им с информаторите на основата на по-дългия им служебен стаж в определена степен подлежат на промяна посредством адекватни и последователни управленски интервенции.

Оказа се, че лоялността на информаторите е базово качество, което мъжете оперативни работници със значителен стаж високо ценят. По-малка тежест в представата им за ценените качества на информаторите имат тяхната наблюдателност, комбинативност, упоритост и готовност за поемане на рискове.

Литература

1. **Асенов,** Б. Теория на разузнаването. София: Албатрос, 2005.
2. **Асенов,** Б. Теория на разузнаването и контраразузнаването. София: Труд, 2012.
3. **Кунчев,** Й. Криминалистика от А до Я. София: Сиела, 2013.
4. **Маджаров,** Е., Й. Андонова-Цветанова, Й. Джавелков. Личностни черти и мотивация на двойния агент. – В: *Бюлетин* на Факултет „Полиция“, бр. 12, 2023, с. 18 – 31.
5. **Начев,** Й. Вербовка и агентура. София: Труд, 2014.

РЕЛАЦИЯТА ФИНАНСОВА СИГУРНОСТ – ЗДРАВНА СИГУРНОСТ

доц. д.м. Емилия Касова
Висше училище по сигурност и икономика – Пловдив

THE RELATION FINANCIAL SECURITY – HEALTH SECURITY

Assos. Prof. Emilia Kasova, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Независимо от липсата на дефиниции в нормативната уредба на понятията „финансова сигурност“ и „здравна сигурност“ са налице взаимодействия между тях, които имат както научнотеоретично, така и практическо значение, поради което те ще бъдат обект на разглеждане в следващото изложение. Докладът има за цел да разгледа релацията, след като се изследва като възможност за групиране на обекти в множества, да се разделят тези обекти в групи на базата на категоризация или класификация. Използвани са публикации по темата на доклада, като са предложени авторови препоръки за усъвършенстване на взаимоотношенията.*

Ключови думи: *релация; финансова сигурност; здравна сигурност*

Abstract: *Despite the lack of definitions in the regulatory framework for the concepts of „financial security“ and „health security“, there are interactions between them that have both scientific and theoretical and practical significance, which is why they will be the subject of consideration in the following presentation. The report aims to examine the relation, after considering it as an opportunity to group objects into sets, to divide these objects into groups based on categorization or classification. Publications on the topic of the report are used, and the author's recommendations for improving the relationships are proposed.*

Key words: *relationship; financial security; health security*

Понятията „финансова сигурност“ и „здравна сигурност“

Независимо от липсата на дефиниции в нормативната уредба на понятията „финансова сигурност“ и „здравна сигурност“ са налице взаимодействия между тях, които имат както научнотеоретично, така и практическо значение, поради което те ще бъдат обект на разглеждане в следващото изложение. Една от основните идеи в областта на концепцията за релация в дискретната математика е, след като се разгледа възможността за групиране на обекти в множества, да се спрем на идеята за разделяне на тези обекти в групи на базата на категоризация или класификация. В нашия конкретен случай релацията финансова сигурност – здравна сигурност означава да класифицираме нещата. Например класифицираме сигурността като състояние на спокойствие и увереност, че няма заплаха или опасност, финансова сигурност, като състояние на финансовия ресурс, обезпечаващ здравните потребности за предоставяне на качествени здравни услуги и здравно обслужване на пациентите. Здравната сигурност на обществото е система от норми, институции, дейности и отношения, целенасочени към максимално възможна равнопоставеност на шансовете на гражданите за гарантиране на тяхното здраве, съответно на достъпа им до здравни услуги с високо качество [1: 7].

Понятието „финансова сигурност“ [3: 24] има различно измерение както на ниво национални икономически агенти (домакинства, фирми и правителство), така и в международен и глобален план, като във всяко едно от посочените измерения има

своето парично (валутно) изражение, измерено в причинени щети и защита на финансовите интереси. Важен елемент на финансовата сигурност се явяват финансовите регулации, които включват предприемане на законодателни мерки, финансови практики и процедури, свързани с гарантиране на сигурността, спокойствието и увереността, че няма да има заплаха или опасност от всички възможни рискови събития, които могат да предизвикат пълна или частична измама и престъпление срещу индивидите, юридическите лица, държавата и глобалния свят, включително и в здравния сектор.

Релацията финансова сигурност – здравна сигурност

Релацията [7] представлява припокриващо съпоставяне между отделни елементи от две или повече множества. Може да се каже, че е налице релация между финансовата сигурност и здравната сигурност като съставни части на системата на националната сигурност в тесен смисъл на думата, включващ тези два елемента, и в широк смисъл, включващ освен тях, и финансовия контрол. Между разглежданите елементи – финансовата сигурност и здравната сигурност, се установява припокриващо съпоставяне при осъществяването на контролната дейност. Отчасти контролът се припокрива с извършвания одит в публичния сектор, който е независима и обективна дейност за предоставяне на увереност и консултиране, предназначена да носи полза и да подобрява дейността на организацията, докато вътрешният финансов контрол обхваща цялостно дейността на административната структура, като основната цел е да се оцени състоянието на вътрешния контрол и ръководството да получи увереност, че извършваните контролни дейности функционират според предназначението си и остават ефективни във времето.

Финансовото управление в здравеопазването, основано на технологиите с изкуствен интелект, носи предимства, които произтичат от натрупването на по-пълен набор от знания, от рационализирането на процеса и елиминирането на емоционалната нестабилност при взимането на решения, от преорентирането от рутинност на дейностите и неудовлетворителност от определени повтарящи се работни задачи към друг тип, по-творчески дейности, от разширяването на обхвата и мащаба на действие, от разрешаването на по-комплексни проблеми за по-кратко време и т.н. Резултатите от подобно управление надхвърлят спестяването на разходи, постигат се оперативна ефективност и натрупване на икономии от мащаба и ефекти от опита. И не по-маловажно – получават се и по-добри познания за начините на бизнес развитие и организационно усъвършенстване, както и по-голяма увереност за разширяване на здравната дейност на нови и чужди места. Тази материя се нуждае от по-специално задълбочено изследване [8: 12].

Пандемията от Ковид-19, която в продължение на повече от три години убиваше милиони хора, допринесе за ускоряването на съществуващите процеси на цифровизация и цифрова трансформация, за възхода на роботиката и преминаването към следващия етап в индустриалното развитие – Индустрия 5.0. От една страна, наличните технологии започват да се прилагат още по-активно, за да се управляват ефектите от пандемията, а от друга, дава се допълнителен тласък на техническия прогрес чрез дигиталната трансформация и финансовата сигурност, които неизменно се отразяват на публичните финанси, и преди всичко на косвеното облагане като приоритетно по отношение на данъчните приходи в държавния бюджет [4: 96; 5: 121]. Във връзка с това, за да запази или подобри конкурентните си позиции в новата ситуация, при здравните услуги трябва да се прилагат технологиите, да се въвеждат разнообразни иновации и да се адаптират бизнес моделите. На новия етап на технологичен

напредък все повече се откроява значението на нововъзникващите, в т.ч. на когнитивните, технологии, и по-конкретно на изкуствения интелект, което насочва дискусията към съответните им приложения в здравеопазването, към здравните проблеми, които се решават с тяхна помощ, към ефективността им за здравните резултати и ползите от прилагане на подобни иновации. Несъмнено компаниите, които са насочени към подобряване на здравните услуги, са изправени пред постоянно предизвикателство да откриват, привличат и интегрират ресурси, да оптимизират дейностите си (бизнес процесите). Това от своя страна е обвързано с управленски знания, умения и способности за наблюдение и диагностика на бизнес средата, за да може здравното заведение да се възползва от протичащите в него промени и тенденции.

В световен мащаб хуманната медицина цели профилактика на заболяванията, диагностика, лечение, рехабилитация и предотвратяване на риска за здравословното състояние на хората. Тя играе изключително важна роля за укрепване на здравето и трудоспособността на населението и допринася за икономическото и социалното развитие на всяка една държава, която е приела развитието с данъчни регулации и повишаване на сигурността си [6: 982].

Здравната сигурност се явява „подсистема на системата за национална сигурност и има непрекъснато взаимодействие с останалите подсистеми на сигурността, играе основна роля за възпроизводството в количествен и качествен аспект на човешкия фактор и за социално-икономическото развитие в контекста на предизвикателствата на динамичните промени на средата за сигурност и на социалната среда“ [2: 45]. Възприема се също така като система от норми, институции, дейност и отношения, насочени към максимално възможна равнопоставеност за гарантиране на здравето и достъпа на гражданите до здравни услуги с високо качество. Здравната сигурност [10: 23] е основен приоритет както на Европейския съюз, така и на всяка държава членка, поради това действа засилен общ координиран подход за противодействие на заплахите за живота и здравето на населението.

В изследването в доклада приоритетен характер имат проблемите на икономиката на здравеопазването, свързани с институциите и с инструментите на финансирането на здравните услуги, и отношението им към финансовата и здравната сигурност. Главният аргумент за възприемането на подобен подход е типичната за нашата страна финансова зависимост в сферата на здравеопазването от здравните вноски от трудовата заетост на населението (задължителното здравно осиуряване), доброволното (частното) здравно осигуряване и здравното застраховане. Промяната в здравната политика е свързана с реформиране на здравната система в страната, което изисква и се очаква създаване на високо качество на медицинското равнище на здравните услуги при ограничаване на разходите за здравеопазване в сферите, в които това е наложително, за сметка на увеличението в останалите сфери.

Налице са нерешени здравни проблеми, които имат различен характер. Кадровата обезпеченост е проблем, който все повече и повече ще се задълбочава в бъдеще. Необходимо е да се провежда активна държавна политика за задържането и обучаването на кадри в здравеопазването, които да обезпечат нуждите на системата. Наблюдава се огромната опасност голяма част от специалностите да останат без достатъчно кадри. За решаването на този проблем е необходимо да се вземат мерки, които да осигурят ясни правила и прозрачна система на следдипломна квалификация на лекарите, която да е предпоставка за достоен и пълноценен живот. Задържането на младите кадри в България е необратимо свързано и с извършването на реформи в целия сектор, защото най-важното за младите лекари е те да виждат пред себе си перспектива; ясни

правила, които стимулират работата и знанието; ясни перспективи за развитие и обучение през целия професионален живот; реална инфраструктура, която да обезпечи нормален процес на обучение и работа.

Финансирането в здравната система също е проблем, който винаги е предизвиквал много дискусии и мнения. Здравеопазването е сектор, който изисква огромен финансов ресурс. Затова са необходими ясни разчети и правила за прозрачно финансиране на сектора. Необходимо е преосмисляне на модела на финансиране. Настоящият монопол на НЗОК не осигурява адекватно оползотворяване на средствата. Необходими са реформи, които да доведат до реална конкуренция в сектора на здравно осигуряване, за да може всеки пациент като гражданин да знае и да вярва, че ще получи възможно най-добрата здравна грижа.

Известно е, че здравеопазването е консервативна система, в която трудно се осъществяват промени, и именно поради това необходимите стъпки трябва да се извършат смело, за да може в недалечно бъдеще да имаме система на здравеопазване, която да осигурява здравето и достойнството на гражданите, която работи в техен интерес и осигурява адекватно професионално развитие на кадрите, които работят в нея [9: 83].

Анализът на дейността и тенденциите на развитие показват, че въпреки сложната обществено-икономическа ситуация лечебните заведения ще продължат да се развиват с устойчиви темпове и реалистични резултати, с предоставяне на модерна и висококвалифицирана медицинска услуга, като по този начин ще отговорят на постоянно нарастващите изисквания за подобряване на релацията финансова сигурност – здравна сигурност.

Литература

1. **Борисов,** В. Здравен мениджмънт с основи на здравната политика. София: Филвест, 2003.
2. **Коев,** К. Здравеопазване и национална сигурност. Монография. София: За буквите – О писменехъ, 2018.
3. **Петев,** Б. Финансова сигурност. Пловдив: ВУСИ, 2024.
4. **Петев,** Б. Необходимост от разширяване на обхвата на данъчното облагане. – В: *Годишник* на ВУСИ, том XXI, 2024, Пловдив, 2025, с. 96.
5. **Петев,** Б. Проблемите на облагането на косвените данъци – тест за публичните финанси. – В: *Годишник* на ВУСИ, том XXI, 2024, Пловдив, 2025, с. 121.
6. **Петрова,** Н. Данъчни регулации и сигурност. – В: *Сборник* с доклади от Годишна университетска научна конференция, 30.06 – 1.07.2022 г., Велико Търново: НВУ „Васил Левски“, 2022, с. 982.
7. ***Уикипедия*** – свободна енциклопедия.
8. **Хаджичонева,** Ю. Предприемачество, иновации и изкуствен интелект в България & динамика и управление. София: УНСС, 2022.
9. **Язов,** К. Общественото достояние на информацията и влиянието ѝ върху сигурността на обществото. София: Военна академия „Георги Стойков Раковски“, 2023.
10. **Kasova,** E. Improving the organization and management of funding as a factor for health security. – В: *Българско* списание за обществено здраве, том 15, кн. 3, Издание на Националния център по обществено здраве и анализи, София, 2023, с. 23.

ПРЕВЕНЦИЯ И ПРОТИВОДЕЙСТВИЕ СРЕЩУ ИЗПИРАНЕТО НА ПАРИ В ОБЛАСТТА НА ХАЗАРТА – ВЗАИМОДЕЙСТВИЕ МЕЖДУ ФИНАНСОВОТО РАЗУЗНАВАНЕ, ДАНС И НАП И СИГУРНОСТТА НА ДЪРЖАВАТА

доц. д-р Недялка Петрова
Висше училище по сигурност и икономика – Пловдив

PREVENTION AND COUNTERACTION AGAINST MONEY LAUNDERING IN THE FIELD OF GAMBLING – INTERACTION BETWEEN FINANCIAL INTELLIGENCE, THE STATE AGENCY FOR NATIONAL SECURITY (SANS) AND THE NATIONAL REVENUE AGENCY (NRA) AND STATE SECURITY

Assoc. Prof. Nedyalka Petrova, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Докладът разглежда изпирането на пари като заплаха и отражение върху националната сигурност. Разглеждат се проблемите и предизвикателствата при взаимодействието между Специализираната административна дирекция „Финансово разузнаване“ на ДАНС и НАП като контролни органи в тази област.*

Ключови думи: *хазарт; финансова сигурност; национална сигурност; Национална агенция за приходите; Специализирана административна дирекция „Финансово разузнаване“ на Държавната агенция „Национална сигурност“*

Abstract: *The report examines money laundering as a threat and impact on national security. It examines the problems and challenges in the interaction between the Specialized Administrative Directorate „Financial Intelligence“ of the State Security Service and the National Revenue Agency as control bodies in this area.*

Key words: *gambling; financial security; national security; National Revenue Agency; Specialized Administrative Directorate „Financial Intelligence“ of the State Agency „National Security“*

Увод

Изпирането на пари е проблем, който засяга не само финансовата система на една държава, но и нейната национална сигурност. В България превенцията и противодействието срещу изпирането на пари в областта на хазарта се осъществява чрез сътрудничество между различни държавни органи, включително Националната агенция за приходите (НАП) и Специализираната административна дирекция „Финансово разузнаване“ (САД ФР) към Държавната агенция „Национална сигурност“ (ДАНС).

Приходите за държавата от хазартна дейност нарастват ежегодно, като бързата дигитализация на сектора прави пазара все по-иновативен и динамичен, което пък води и до по-големи рискове, свързани с хазартната дейност, и повишаване на изискванията, квалификацията и бързината на осъществявания контрол.

През последните години хазартният бранш претърпя голямо развитие. Това се усеща и от постъпленията в бюджета. Според данни на Асоциацията на игралната индустрия в България (АИИБ), базирани на информация от НАП, приходите от игралната индустрия в България за 2024 г. са в размер на 392 340 915 лв. Секторът остава стабилен източник на бюджетни приходи въпреки затварянето на част от игралните

зали. Според данни на АИИБ с добавяне на сумата от събрания алтернативен данък по ЗКПО приходите надхвърлят 490 млн. лв.

Към 8.01.2025 г. в страната оперират 21 игрални казина и 1082 игрални зали с игрални автомати, като няма действащи обекти за числови лотарийни игри, като Бинго и Кено. Онлайн хазартният сегмент продължава да се разраства, като броят на лицензираните оператори достига 51. В страната функционират 2183 букмейкърски пункта, 6 лицензирани оператора за наземни спортни залози и 53 производители на игрално оборудване [4].

През миналата година българите са спечелили от хазартни игри близо 1,4 млрд. лв., а направените залози в игри на късмета са около 2,8 млрд. лв., показват изчисления на „Труд news“ на базата на данни на Националната агенция за приходи за събраните в държавния бюджет средства от хазартния бранш [8].

Хазартът се свързва с незаконни действия, като пране на пари, укриване на данъци, разпространение на наркотици, финансиране на тероризма и др., които засягат пряко националната сигурност на всяка една държава. Поради това е необходимо строго регулиране на тази дейност. Участието в хазартни игри може да доведе и до сериозни последици, включително опасност от пристрастяване. В тази връзка съгласно чл.10а, ал. 4 от ЗХ по бюджета на Министерството на младежта и спорта се предвиждат и разходват средства за финансиране на одобрени проекти за младежки дейности.

В близкото минало много често прането на пари ставаше през хазартни игри – чрез залагания в електронни сайтове на резултати от футболни срещи или в казина. Промените в Закона за хазарта (ЗХ) имаха за цел да ограничат до минимум тези практики. Всеки игрален автомат и рулетка вече са вързани директно с НАП и има информация какви са оборотите на машините. Освен това печалби над 5000 лв. се изплащат само по банков път.

Взаимодействие между Специализираната административна дирекция „Финансово разузнаване“ на ДАНС и НАП в превенцията и противодействието срещу изпирането на пари в областта на хазарта – особености и ред за извършване на съвместни проверки

Още през 2013 г. Европейската комисия се насочи към противодействие срещу изпирането на пари в областта на хазарта през сайтовете за онлайн залагане, като предвиди, че в законодателството, освен казината, трябва да бъдат включени и интернет страниците, които предлагат такъв вид хазарт, и официално предложи тези сайтове да станат обект на законите за борба срещу измамите. Според комисията, упражнявайки контрол само върху казината, другите видове хазарт стават уязвими откъм злоупотреби и пране на пари.

Беше приета Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20.05.2015 г. за предотвратяване на използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, която се прилага и по отношение на доставчици на хазартни услуги и има за цел да укрепва и подобрява сътрудничеството между звената за финансово разузнаване (ЗФР), които са сред основните участници в борбата срещу изпирането на пари/финансирането на тероризма. Систематичният обмен на информация между ЗФР трябва да се осъществява чрез напреднала техническа инфраструктура с помощта на FIU.net – децентрализирана компю-

търна мрежа, която използва усъвършенствана технология за намиране на съответствия. С нея е предвидено, че съмненията за изпиране на пари или финансиране на тероризма трябва да бъдат докладвани на публичните органи, обикновено на ЗФР.

Съгласно Директивата изпирането на пари е преобразуването на приходите от престъпления в привидно чисти средства, обикновено чрез финансовата система, например чрез прикриване на източниците на парите, промяна на формата им или прехвърляне на средствата на място, където е по-малко вероятно те да привлекат внимание.

Финансоворазузнавателно звено на Република България е Специализираната административна дирекция „Финансово разузнаване“ при Държавна агенция „Национална сигурност“ (САД ФР – ДАНС), която получава, съхранява, проучва, анализира и разкрива получената при спазване на реда и условията на Закона за мерките срещу изпирането на пари (ЗМИП) и Закона за мерките срещу финансирането на тероризма (ЗМФТ) информация. САД ФР – ДАНС упражнява и контрол за спазване на изискванията на ЗМИП, ЗМФТ и актовете по прилагането им от страна на задължените субекти по чл. 4 от ЗМИП.

През януари 2020 г. България обяви завършването на първата си цялостна Национална оценка на риска (НОР) от изпиране на пари и финансиране на тероризъм. Тази оценка се извършва в съответствие с методиката на Групата за финансови действия срещу изпирането на пари (FATF) и Комитета на експертите за оценка на мерките срещу изпирането на пари (Комитета MONEYVAL) към Съвета на Европа. Непрекъснатото развитие на заплахите и уязвимостите в това отношение налага периодичната актуализация на Националната оценка на риска.

С изменение на Закона за хазарта, *ДВ,* бр. 69 от 4.08.2020 г., законодателят вмени държавният надзор в областта на хазарта и свързаните с него дейности да се осъществява от изпълнителния директор на НАП или упълномощен от него заместник изпълнителен директор, като съответно ЗМИП определя НАП като надзорен орган. НАП заедно със САД ФР – ДАНС осъществява контрол над тези две категории задължени лица по смисъла на чл. 4 от ЗМИП за спазване на изискванията на ЗМИП, ЗМФТ и актовете по прилагането им. Ако при осъществяване на надзорната си дейност органите по приходите в НАП установят факти и обстоятелства, които е възможно да са свързани с изпиране на пари, незабавно следва да уведомят САД ФР – ДАНС [7].

Контролните действия по прилагането на ЗМИП и ЗМФТ се осъществяват комплексно в хода на данъчно-осигурителния контрол от органите по приходите в Дирекция „Контрол“ и Главна дирекция „Фискален контрол“ в НАП. И тази проверка е задължителна при всяко контролно производство по Закона за хазарта.

От 1.06.2023 г. в НАП бе създаден отдел „Превенция и противодействие срещу изпирането на пари“ в Дирекция „Надзор върху хазарта и хазартните дейности“. Правомощията на новото звено е да координира, наблюдава и подпомага изпълнението на дейността, осъществявана от органите по приходите, съгласно ЗМИП, ППЗМИП и ЗМФТ.

В тази връзка НАП разработи **Методически указания с изх. № 93-00-4098/18.08.2023 г. за прилагане на разпоредбите на ЗМИП и ЗМФТ от организаторите на хазартни игри** на територията на Република България, съгласно които:

На основание на чл. 3, т. 1 – 8 от ЗМИП мерките за превенция на използването на финансовата система за целите на изпирането на пари, които организаторите на хазартни игри (ОХИ) задължително следва да спазват, са изчерпателно изброени, а именно:

1. комплексна проверка на клиентите;

2. събиране и изготвяне на документи и друга информация при условията и по реда на този закон;

3. съхраняване на събраните и изготвените за целите на този закон документи, данни и информация;

4. оценка на риска от изпиране на пари и финансиране на тероризма;

5. разкриване на информация относно съмнителни операции, сделки и клиенти;

6. разкриване на друга информация за целите на този закон;

7. контрол върху дейността на задължените субекти по Раздел II от тази глава;

8. обмен на информация и взаимодействие на национално равнище, както и обмен на информация и взаимодействие между Дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“, звената за финансово разузнаване на други държави и юрисдикции, както и с компетентните в съответната сфера органи и организации на други държави.

Организаторите са длъжни съгласно чл. 14 от ЗМИП да прилагат мерките за комплексна проверка по чл. 10 при всеки случай на съмнение за изпиране на пари и/или за наличие на средства с престъпен произход независимо от стойността на операцията или сделката, рисковия профил на клиента, условията за прилагане на мерките за комплексна проверка или други изключения, предвидени в този закон или в правилника за прилагането му.

Общите правила за прилагане на мерките за комплексна проверка са посочени в чл. 11 от ЗМИП, като в чл. 10, т. 1 – 5 от ЗМИП е посочено какви действия включва комплексната проверка на клиента, като ОХИ е необходимо да ги изследва изчерпателно.

Разпоредбата на чл. 12 от ЗМИП определя основното правило за прилагане на мерките за извършване на комплексна проверка на клиента от страна на ОХИ при:

1. вписването в регистъра по чл. 74, ал. 1 от Закона за хазарта;

2. изплащането на печалби и/или осъществяването на залагания на обща стойност, равна или надвишаваща левовата равностойност на 2000 евро или тяхната равностойност в друга валута, независимо дали операцията или сделката е осъществена чрез една операция, или чрез няколко свързани операции;

3. покупка, обмен или осребряване на жетони или други удостоверителни знаци за потвърждаване на печалбата на обща стойност, равна или надвишаваща левовата равностойност на 2000 евро или тяхната равностойност в друга валута, независимо дали операцията или сделката е осъществена чрез една операция, или чрез няколко свързани операции.

При прилагането на чл. 12 от ЗМИП следва да се има предвид разпоредбата на § 1, т. 14, б. „а“ от ДР от ЗМИП, съгласно която „Свързани операции“ са операциите и сделките, които представляват поредица последователни прехвърляния на парични средства или ценности от или на едно и също физическо лице, юридическо лице или друго правно образувание, които са извършени във връзка с едно задължение, когато всяко отделно прехвърляне е под законовия праг, но които заедно отговарят на критериите за прилагане на мерките за комплексна проверка, или поредица прехвърляния чрез различни лица по чл. 4, която е свързана с едно и също задължение, или друга свързаност, установена с оглед на спецификата на операциите или сделките, основана на прилагане на мерките по този закон.

Идентифицирането на клиентите и проверката на идентификацията се извършва въз основа на документи, данни или информация, получени от надеждни и независими източници по реда на чл. 53 и чл. 54 от ЗМИП.

ОХИ поддържат актуална събраната чрез прилагането на мерките за комплексна проверка информация за своите клиенти и за извършваните от тях операции и сделки, като периодично преглеждат и актуализират при необходимост поддържаните бази данни и клиентски досиета, като прилагат мерките за комплексна проверка,

включително когато на лицето по чл. 4 стане известно, че е настъпила промяна в обстоятелствата по отношение на клиента (чл. 16 от ЗМИП).

Разпоредбата на чл. 35 от ЗМИП посочва случаите, в които се прилагат мерки за разширена комплексна проверка по реда на Глава втора, Раздел IV от ЗМИП и Правилника за прилагане на закона.

Една от важните проверки, които следва да извърши ОХИ, се отнася до **идентифициране на видни политически личности,** като те са изчерпателно изброени в чл. 36 от ЗМИП. Всички процедури по отношение на видни политически личности се прилагат и за членовете на техните семейства и близките им сътрудници в качеството на „свързани лица“. За встъпване на лице по чл. 4 в делови взаимоотношения с лица, за които е установено, че са лица по чл. 36, се изисква одобрение от служител на висша ръководна длъжност на лицето по чл. 4.

Методите за установяване дали е налице видна политическа личност, са дадени от чл. 42, ал. 2 от ЗМИП. Тези методи са:

• информация, получена чрез прилагане на мерките за разширена комплексна проверка;

• писмена декларация, изискана от клиента, с цел установяване дали лицето попада в някоя от категориите по чл. 36;

• информация, получена чрез използването на вътрешни или външни бази данни.

Писмената декларация по чл. 42, ал. 2, т. 2 от ЗМИП следва да съдържа реквизитите съгласно Приложение 1 към чл. 26, ал. 1 от ППЗМИП.

ППЗМИП допуска тази декларация да бъде включена като част от друг документ, изходящ от декларатора, но трябва да съдържа всички реквизити на Приложение № 1 към чл. 26, ал. 1 от ППЗМИП и да не предизвиква съмнение за лицето, което я подава и относно съдържанието ѝ.

В Глава втора, Раздел VII, чл. 66 на ЗМИП са посочени способите за прилагане при изясняване на произхода на средствата, като ОХИ следва да прилагат поне два от посочените в чл. 66, ал. 1 способи. При невъзможност за изясняване на произхода на средствата след изчерпване на способите по чл. 66, ал. 1 от ЗМИП, както и в случаите, при които прилагането на поне два от тях е довело до противоречива информация, изясняването на произхода на средствата се извършва чрез изискване на писмена декларация от клиента или от неговия законен представител/пълномощник, която е по образец – Приложение № 4 към чл. 47, ал. 1 от ППЗМИП. Следва да бъде отбелязано, че към тази възможност следва да се подхожда само след използване на поне два от посочените в чл. 66, ал. 1 способи и не е постигнато изясняване на произхода на средства.

Специално внимание следва да се обърне на разпоредбата на чл. 42, ал. 3 (нова – *ДВ,* бр. 84 от 2023 г.), че установяването дали потенциален клиент, съществуващ клиент или действителен собственик на клиент – юридическо лице или друго правно образувание, е лице по чл. 36, не може да се основава единствено на информация, получена от писмената декларация [6].

При съмнение и/или узнаване за изпиране на пари и/или за наличие на средства с престъпен произход лицата по чл. 4 (в т.ч. и организаторите на хазартни игри, получили лиценз за организиране на хазартни игри на територията на Република България съгласно ЗХ) **са длъжни да уведомят незабавно Дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“** преди извършването на операцията или сделката, като забавят нейното осъществяване в рамките на допустимия срок съгласно нормативните актове, уреждащи съответния вид дейност. В уведомлението лицата следва да посочат максималния срок, в който операцията или сделката може да се отложи. При узнаване за изпиране на пари или за наличие на средства

с престъпен произход лицата по чл. 4 уведомяват и компетентните органи съгласно Наказателнопроцесуалния кодекс, Закона за Министерството на вътрешните работи и Закона за Държавна агенция „Национална сигурност“ (чл. 72, ал. 1 от ЗМИП).

Лицата по чл. 4 **уведомяват Дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“ за всяко плащане в брой на стойност над 30 000 лв.** или тяхната равностойност в чужда валута, извършено от или на техен клиент в рамките на установените отношения или при случайни сделки или операции (чл. 76, ал. 1 от ЗМИП).

За да установят, разберат и оценят рисковете от изпиране на пари и финансиране на тероризма, лицата по чл. 4 изготвят собствени оценки на риска, като отчитат съответните рискови фактори, включително тези, които се отнасят до клиентите, държавите или географските зони, предлаганите продукти и услуги, извършваните операции и сделки или механизмите за доставка (чл. 98 от ЗМИП).

За изготвяне на оценките си на риска по чл. 98 от ЗМИП лицата по чл. 4 от същия закон могат да използват избрана от тях методика и категории рискове от изпиране на пари и финансиране на тероризъм, които включват най-малко категориите на висок, среден и нисък риск (чл. 60, ал. 1 от ППЗМИП).

Оценките на риска на лицата по чл. 98 от ЗМИП се актуализират на всеки две години, както и в случаите по т. 1 – 3 на чл. 60, ал. 5 от ППЗМИП, документират се и се съхраняват по реда на Глава трета, Раздел I за срок 5 (пет) години и са достъпни за Дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“.

ОХИ са задължени да приемат вътрешни правила за контрол и предотвратяване на изпирането на пари и финансирането на тероризма, чието съдържание е изчерпателно изброено в разпоредбата на чл. 101, ал. 2 от ЗМИП.

Лицата по чл. 4 са длъжни да осигуряват въвеждащо и продължаващо обучение на служителите си за запознаването им с изискванията на този закон, ЗМФТ и актовете по прилагането им, както и с вътрешните правила по този член, включително провеждане на текущи програми за обучение, насочени към разпознаване на съмнителни операции, сделки, източници и клиенти и към предприемане на необходимите действия при възникнали случаи на съмнение за изпиране на пари или финансиране на тероризма (чл. 101, ал. 11 от ЗМИП).

ОХИ са длъжни да създадат специализирани служби при условията и по реда на чл. 106 или изпълняват лично вътрешния контрол по изпълнението на задълженията си по ЗМИП и ППЗМИМ (чл. 107, ал. 1 от ЗМИП).

Съгласно чл. 9, ал. 2 от ЗМФТ лицата по чл. 4 от ЗМИП прилагат мерките по чл. 3, т. 1 – 4 от същия закон с оглед на превенцията на използването на финансовата система за целите на финансирането на тероризма при условията и по реда на чл. 5 – 9, Глава втора, Глава трета и Глава седма от ЗМИП и на ЗМФТ [2].

С Инструкция [1] беше уреден и редът за осъществяване на съвместни проверки на място от Специализираната административна дирекция „Финансово разузнаване“ на ДАНС и НАП по прилагането на мерките за превенция на използването на финансовата система за целите на изпирането на пари и финансирането на тероризма по отношение на лицата по чл. 4, т. 21 (организаторите на хазартни игри, получили лиценз за организиране на хазартни игри на територията на Република България съгласно Закона за хазарта) от Закона за мерките срещу изпирането на пари (ЗМИП).

Съвместните проверки се извършват въз основа на писмена заповед, издадена от председателя на ДАНС или от оправомощено от него длъжностно лице и от изпълнителния директор на НАП или от оправомощено от него длъжностно лице, в която се посочват целите, обхватът, срокът и мястото на проверката, проверяваните лица, други обстоятелства от значение за проверката, ако има такива, както и имената и

длъжностите на лицата, на които се възлага да извършат проверката – контролните органи по чл. 108, ал. 2 от ЗМИП и органите по приходите.

Целите на проверките се определят в зависимост от резултатите от прилагането на основан на риска подход по чл. 114, ал. 1 и чл. 115 от ЗМИП или възникналата необходимост за извършване на проверка. С оглед на целите и обхвата за всяка проверка се изготвя план, който съдържа разпределението на отговорностите, темите, предмета на проверката и други изисквания и необходими действия съгласно изискванията на ЗМИП и ЗМФТ между длъжностните лица на двете институции в рамките на техните законоустановени правомощия.

Заповедта за проверка се изготвя в три екземпляра – за САДФР на ДАНС, НАП и проверяваното лице, и се връчва срещу подпис на проверяваното лице ведно с писмо-искане на справки и документи. За всяка извършена проверка на място по чл. 108, ал. 4 от ЗМИП се съставя констативен протокол в три екземпляра, който се подписва от длъжностните лица, извършили проверката, и се връчва срещу подпис на провереното лице. Актовете за установяване на нарушенията се съставят от контролните органи на САДФР на ДАНС и НАП по чл. 123 от ЗМИП и чл. 16 от ЗМФТ в рамките на законоустановените им правомощия и предвиденото в плана по ал. 4 разпределение. Наказателните постановления се издават от председателя на ДАНС или от оправомощено от него длъжностно лице, съответно от изпълнителния директор на НАП или от оправомощено от него длъжностно лице (чл. 5, ал. 3 – 8 от Инструкцията).

При извършваните съвместни проверки се проверяват:

- наличието на изготвени вътрешни правила – как идентифицират видни политически личности; как изясняват произхода на средствата; как определят рисковия профил на клиентите; оценката на риска;

- как се извършва идентификацията на лицата – не са „официални документи за самоличност“ документите за пребиваване и чуждестранното свидетелство за управление на моторно превозно средство. На сайта на МВР може да се провери самоличността на дадено ФЛ във връзка с проверка по ЗМИП;

- софтуерът за проверка на вида политическа личност и по ЗМФТ;

- оценката за риска и дали е съобразена с националната оценка;

- изисква се справка за изплатените печалби и за случаите над 2000 евро отново търсим доказателства за извършена комплексна проверка;

- броят клиенти може да се установи чрез регистър и ПОС, изисква се информация за всички клиенти и как е приложена комплексната проверка;

- справката за трансакциите на постерминал – дали има залог над 2000 евро, иска се идентификация, прилага се комплексна проверка на лицето, изследва се произходът на средствата чрез декларация образец съгласно ППЗМИП. Ако ФЛ посочи спестявания, трябва да посочи и периода, за който са спестени средствата. Декларацията за произход на средствата е приложима и за онлайн хазарта.

Най-честите нарушения от страна на проверяваните лица са: в регистъра по чл. 74, ал. 1 от ЗХ не се извършва коректна идентификация на лицата или не поддържат актуална база данни. Налице е нарушение, когато организаторът на хазартни игри е установил, че ФЛ е видна политическа личност и не е предприел действия да уведоми ДАНС, поради което подлежи на санкция.

Съгласно чл. 74, ал. 2 от ЗХ в казиното организаторът е длъжен да осигури система за непрекъснат видеоконтрол върху игралните маси, игралните автомати, персонала и участниците в игрите.

С оглед на изложеното и актуалната нормативната уредба могат да се направят следните изводи относно ролята на САД ФР към ДАНС и НАП за дейността им, насочена срещу изпирането на пари в областта на хазарта:

1. **Ролята на САД ФР към ДАНС** е да следи финансовите трансакции и операции, които могат да бъдат свързани с изпиране на пари. Това включва наблюдение на съмнителни трансакции в казината, букмейкърите и други хазартни обекти.

Дирекцията събира и анализира данни от различни източници, включително доклади за съмнителни сделки, подадени от хазартните оператори. При наличие на подозрения за изпиране на пари САД ФР може да предприеме необходимите действия за предотвратяване и санкциониране на незаконни дейности.

САД ФР работи и в тясно сътрудничество с международни партньори и организации, като Financial Action Task Force (FATF) и Европейската комисия.

2. **Ролята на НАП** е да контролира спазването на данъчните закони и регулации в хазартния сектор. Това включва проверка на финансовите отчети и данъчните декларации на хазартните оператори.

Изпълнителният директор на НАП издава, отказва да издаде, прекратява и отнема лицензи за организиране на хазартни игри, лицензи за производство, разпространение и сервиз, както и лицензи за внос, разпространение и сервиз на игрално оборудване.

НАП води регистри по чл. 20 от ЗХ, достъпни за всички организатори на хазартни дейности и граждани.

Организаторите на хазартни игри от разстояние (ОХИР) следва да подават информацията през наета линия към информационна система и сървър на НАП, достъп до който е предоставен от НАП индивидуално за всеки организатор на хазартни игри.

Всяко лице, което смята, че има проблем с хазарта, както и лицата, чието социално положение и/или равнище на доходи може да ги направи по-податливи към участие в хазартни игри и развиване на хазартна зависимост, могат да се впишат в Регистър на уязвимите лица (създаден на основание на чл. 10г от ЗХ) с цел забрана или недопускането им до участие в хазартни игри.

НАП събира данъците, дължими от хазартните оператори, което помага за предотвратяване на укриването на доходи и изпирането на пари и има правомощията да налага санкции и глоби при установяване на нарушения, свързани с укриване на данъци или други финансови нередности.

Съгласно чл. 47е, ал. 1 от ЗХ организаторите на хазартни игри, на които е издаден лиценз по реда на този закон, предоставят на НАП информация за размера на изплатените парични и предметни печалби на местни физически лица по смисъла на Закона за данъците върху доходите на физическите лица (ЗДДФЛ), както следва:

1. годишен размер на изплатените печалби, превишаващ 5000 лв. на участник в хазартна игра и годишен размер на изтеглените от него суми, когато участникът има игрална сметка при организатора на хазартни игри;

2. всяка отделно изплатена печалба на участник в хазартна игра в размер, превишаващ 5000 лв., когато участникът няма игрална сметка при организатора на хазартни игри.

Във връзка с данъчното третиране на печалбите, получени от физическите лица – участници във въпросните игри, следва да се има предвид, че съгласно **чл. 13, ал. 1, т. 20 и 21 от ЗДДФЛ не са облагаеми:**

- паричните и предметните печалби, получени от участие в хазартни игри, организирани с лиценз, издаден по реда на ЗХ или съгласно законодателството на друга държава – членка на Европейския съюз (ЕС), или държава – страна по Споразумението за Европейското икономическо пространство (ЕИП). Данъчният закон не съдържа собствена дефиниция на понятието „хазартна игра“, поради което за целите на цитираната разпоредба следва да се ползва дадената в ЗХ;

- наградите, които се дават във вид на допълнителна игра или предметна печалба с незначителна стойност от развлекателни автомати, по смисъла на ЗХ или съгласно законодателството на друга държава – членка на ЕС, или държава – страна по Споразумението за ЕИП, както и предметните печалби с незначителна стойност от други игри на случайността, извън посочените в чл. 13, ал. 1, т. 20 от ЗДДФЛ. Съгласно § 1, т. 62 от ДР на ЗДДФЛ предметни печалби с незначителна стойност са тези, чиято пазарна цена е до 100 лв.

Печалбите от игри, които не попадат в обхвата на цитираните разпоредби, представляват облагаем доход по смисъла на данъчния закон. На основание на чл. 38, ал. 14 от ЗДДФЛ брутната сума на придобитите облагаеми парични и предметни награди от игри, от състезания и конкурси, които не са предоставени от работодател или възложител, се облага с окончателен данък. За изплащането на печалбата следва да се издаде първичен счетоводен документ, съответно данните за определяне на печелившите участници и изплащането на дължимото към тях следва да са подкрепени с достоверни други документи, съдържащи необходимата информация (например при онлайн игри това биха могли да бъдат справки от информационната система на хазартния оператор, придружени с платежни документи за превода на дължимата сума към платежната сметка на участника).

Всяка сума пари, достигнала до участниците през централна компютърна система (ЦКС) като директен резултат от хазартните игри, следва да се третира като печалба, т.е. всички реални средства, постъпили в игралните сметки на участниците, следва да се докладват като такава [3].

В Становище с изх. № 24-39-53/20.07.2018 г. на НАП е посочено, че ЦКС захранва игралната сметка на участника с всички негови печалби и допуска той да изтегли всички средства по игралната си сметка. В момента, в който игралната сметка на участника се захрани с печалба, той може да я изтегли или да направи нов залог с нея (иначе казано, вече решение на самия играч е дали да изтегли печалбата, или да я заложи отново). Това още веднъж показва, че получените печалби са реални парични средства, които са предоставени на играчите, и следва да бъдат декларирани като такива в декларацията по чл. 30, ал. 8 от ЗХ [5].

3. **НАП работи в тясно сътрудничество и взаимодействие със САД ФР,** като споделя информация и координира усилията за борба с изпирането на пари. Двете институции обменят информация относно съмнителни трансакции и случаи на потенциално изпиране на пари. Когато се установи случай на изпиране на пари, САД ФР и НАП координират своите действия, за да осигурят ефективен контрол и санкциониране на нарушителите. Съществува риск, когато получената от извършения контрол информация не е оценена правилно.

И двете институции участват в обучения и семинари, насочени към повишаване на осведомеността и квалификацията на служителите в хазартния сектор относно рисковете и методите за предотвратяване на изпирането на пари.

Заключение

Прането на пари застрашава сериозно финансовата сигурност на всяка държава, защото е процес на прикриване на незаконни приходи (от трафик на наркотици, трафик на хора и измами и др.) като законни доходи. Обикновено това се осъществява чрез поредица трансакции, които затрудняват проследяването на произхода на средствата.

Нито един държавен орган не може да се справи сам с рисковете за националната сигурност. Така и тук, в сферата на пране на пари, това се случва чрез ефективното взаимодействие между САД ФР и НАП, което има значителен ефект върху финансовата сигурност на държавата.

По-добър контрол и надзор върху хазартните операции води до повишена прозрачност и намаляване на възможностите за изпиране на пари. Предотвратяването на изпирането на пари защитава обществените интереси и гарантира, че приходите от хазартни дейности се използват законно и справедливо.

Ефективната борба с изпирането на пари укрепва международното доверие в българската финансова система и я прави по-привлекателна за инвестиции, защото прането на пари засяга както вътрешната, така и външната национална сигурност.

В заключение, сътрудничеството между САД ФР и НАП е изключително важно за успешното противодействие на изпирането на пари в областта на хазарта и за поддържането на финансовата сигурност на държавата.

Литература

1. **Инструкция** за реда за извършване на съвместни проверки на място по чл. 108, ал. 4 от ЗМИП от Специализирана административна дирекция САДФР на ДАНС и НАП. [онлайн]. *https://old.nra.bg/document?id=20860.*
2. **Методически** указания от НАП с изх. № 93-00-4098/18.08.2023 г. за прилагане на разпоредбите на ЗМИП и ЗМФТ от организаторите на хазартни игри. [онлайн]. *https://pris.government.bg/document/a6571c43fa1fd1dc3bd5e15b0a91ce76/8066f31e2114ac5acffe90d1ee5eb944.*
3. **Писмо** на НАП с изх. № 26-Т-169/30.06.2023 г. относно третиране на предоставяните от организаторите на хазартни игри бонуси при организираните от тях бонус игри. [онлайн]. *https://old.nra.bg/page?id=381.*
4. **Приходите** от хазартния сектор надхвърлиха 490 млн. лева през 2024 г. [онлайн]. [достъпен 6.04.2025]. *https://agib.bg/bg/prihodite-ot-hazartniya-sektor-nadhvarliha-490-mln-leva-prez-2024-g/.*
5. **Решение** № ППН-01-414/19.09.2020 г. на Комисията за защита на личните данни. [онлайн]. *https://cpdp.bg/.*
6. **Становище** с изх. № М-92-00-1300/23.05.2024 г. относно прилагане на разпоредбите на ЗМИП и ППЗМИП при идентификация и установяване на клиент като видна политическа личност (ВПЛ) или свързано лице с такава личност от организаторите на хазартни игри, получили лиценз за организиране на хазартни игри на територията на Република България. [онлайн]. *https://nra.bg/wps/portal/nra/zakonodatelstvo/drugi-normativni-i-podnormativni-aktove/75ddc98f-e720-4969-bbcf-dba1ca396a45.*
7. **Стратегия** за противодействие на изпирането на пари и финансирането на тероризма в Република България – 2023 – 2027 г. [онлайн]. [достъпен 7.04.2025]. *https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1637.*
8. **Хазартът** е любимият бизнес на българите. [онлайн]. [достъпен 6.04.2025]. *https://trud.bg/a/articles/хазартът-е-любимият-бизнес-на-българите.*

ЕТИЧЕСКИ И ПРАВНИ АСПЕКТИ НА ДЕЙНОСТТА НА БЪЛГАРСКОТО РАЗУЗНАВАНЕ И КОНТРАРАЗУЗНАВАНЕ

доц. д-р Атанаска Тунтова
Висше училище по сигурност и икономика – Пловдив

ETHICAL AND LEGAL ASPECTS OF THE ACTIVITIES OF BULGARIAN INTELLIGENCE AND COUNTERINTELLIGENCE

Assoc. Prof. Atanaska Tuntova, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Службите за сигурност, не само военните, претърпяват реформи през последните години на демократичен преход и съответно реорганизация на дейностите, които изпълняват. Разузнаването включва активни действия, насочени към събиране, натрупване и обработка на ценна информация, забранена за достъп на трети лица, в т.ч. и научно-технически шпионаж. То може да бъде легално и етично разузнаване, когато използва открити източници, но конкуренцията и други външни фактори могат да повлияят негативно и това да доведе до промяна на фокуса на действие. Тук е необходимо да се отчете фактът, че всички дейности се извършват от хора, които понякога са подвластни на събития извън законовите норми. Къде обаче е границата на действие на служителите от разузнаването и контраразузнаването, които са носители на информация, която може да се използва за действия, нарушаващи моралните устои и етическите норми на практика? Възможно ли е носителите на важна информация да се поддадат на различни „изкушения“ и да работят за интересите на конкурентите, в ущърб на собствената си организация, пък било то и в минало време?*

Ключови думи: *разузнаване; контраразузнаване; етически норми; правни норми в разузнаването*

Abstract: *Security services, not only the military, have undergone reforms in recent years of democratic transition and, accordingly, reorganization of the activities they perform. Intelligence includes active actions aimed at collecting, accumulating and processing valuable information, prohibited for access by third parties, including scientific and technical espionage. It can be legal and ethical intelligence when it uses open sources, but competition and other external factors can have a negative impact and this can lead to a change in the focus of action. Here it is necessary to take into account the fact that all activities are carried out by people who are sometimes subject to events outside the legal norms. However, where is the limit of action for intelligence and counterintelligence officers, who are carriers of information that can be used for actions that violate moral foundations and ethical norms in practice? Is it possible for holders of important information to succumb to various „temptations“ and work for the interests of competitors, to the detriment of their own organization, even in the past tense?*

Key words: *intelligence; counterintelligence; ethical norms; legal norms in intelligence*

Въведение

Разузнавателните и контраразузнавателните служби в България имат основополагаща роля в защитата на националната сигурност, но тяхната дейност неизбежно поражда сложни етически и правни въпроси. В епоха на нарастващи глобални заплахи и технологичен напредък доверието в тези институции зависи от способността им да балансират сигурността с принципите на прозрачност и законност. Един особено чувствителен проблем е свързан с преминаването на служители от разузнавателните служби към други работни места, където съществува риск те да използват поверител-

ната информация, натрупана по време на службата си, в полза на новите си работодатели. Този доклад цели да се анализират правните и етическите аспекти на дейността на българските разузнавателни служби с акцент върху рисковете, свързани със смяната на работното място от служители, като разглежда какви предизвикателства възникват и как те могат да бъдат адресирани. Въпросите, които ще бъдат разгледани, включват правните рамки, етическите дилеми и конкретните рискове, свързани с използването на информация след напускане на службите.

В съвременния контекст на глобални заплахи и технологичен напредък етическите и правните рамки са от съществено значение за поддържане на доверието в службите и предотвратяване на злоупотреби.

Днес, въпросите за баланса между националната сигурност и защитата на гражданските свободи са изключително актуални. Разузнавателните служби често оперират в сиви зони, където етическите и правните граници могат да бъдат размити. Изследването на тези аспекти е от ключово значение за разбирането на ролята на разузнаването в демократичното общество.

През годините на преход се създаде идеята за реформи в сектора за сигурност на страната, което би било добре от гледна точка да се отговори на съвременните предизвикателства, но всъщност в каква степен структурите и служителите са готови за това. Какво обхваща секторът за сигурност? Могат да се разгледат различни аспекти на сигурността, но един от съвременните възгледи е, че секторът за сигурност включва организациите и структурите за сигурност, т.е. полицията, въоръжените сили, разузнавателните и контраразузнавателните служби. През последните години непрекъснато се говори за това, че предстоят реформи в сектора за сигурност, и сякаш това е само едно добро пожелание, а реални действия няма.

Реформата е затруднена от факта, че съществуват разнопосочни и противоречиви цели и интереси на отделни социални групи. Съществено значение за липсата на ясна визия за бъдещето на специалните служби има разглеждането им през първите години на прехода повече като репресивни органи на предишния режим, отколкото като специфични информационни структури, осигуряващи националната сигурност на страната [11: 133].

След повече от 35 години на преход усещането на обществото е, че този модел на работа на службите се запазва в много голяма степен и е в услуга на всяко управление според нуждите на властта. В търсене на отговори относно реформата в службите ще разгледам следните въпроси, които намирам за логични.

Какви са правните и етическите предизвикателства пред службите? Какви рискове възникват при използване на поверителна информация в нови работни среди и как могат да бъдат ограничени?

Правни рамки на дейността на българското разузнаване и контраразузнаване

Дейността на българските разузнавателни служби е регулирана от строги нормативни актове, които определят техните правомощия и задължения. Законът за Държавна агенция „Разузнаване“ (обн. *ДВ,* бр. 79 от 13.10.2015 г.) [9] например установява основните принципи на работа на службата, включително защитата на класифицирана информация. Този закон изрично задължава служителите да спазват конфиденциалност, като предвижда тежки санкции за разкриване на държавни тайни дори след прекратяване на трудовите им отношения. Подобни разпоредби са заложени и в Закона за специалните разузнавателни средства (обн. *ДВ,* бр. 95/1997 г.) [10], който

урежда използването на технически средства за събиране на информация и налага ограничения върху разпространението ѝ.

Контролът върху спазването на тези правила е поверен на институции, като Народното събрание и съдебната система. Парламентарната комисия по вътрешна сигурност и обществен ред периодично преглежда дейността на службите, но нейните правомощия често са критикувани като недостатъчни за ефективен надзор, особено що се отнася до бивши служители.

Ежегодно Държавна агенция „Национална сигурност“ (ДАНС) представя свой годишен доклад за дейността на Агенцията, откъдето всеки може да се запознае с дейността без последните години, тъй като са засекретени. От извършените проверки, в т.ч. и по сигнали, са разкрити корупционни прояви на лица, заемащи висши държавни длъжности. От направен преглед на докладите между 2015 и 2020 г. [2; 3; 4; 5; 6; 7], които са публични, става ясно, че корупционните схеми често включват освен лица, заемащи висши държавни длъжности, и служители на по-ниско йерархично ниво. От анализа на данните от работата на ДАНС се потвърждава трайна тенденция, че към корупционни практики са най-податливи секторите със значителен материален ресурс и където са налице слабости при упражняване на контролни или разрешителни функции.

Пак от докладите на ДАНС става ясно, че са установени и лица, в т.ч. от службите за сигурност, които са разкрили информация, станала им известна по време на заемана длъжност, подлежаща на специален режим по отношение на достъп на информация. Например случай от 2015 г., когато бивш служител на Държавна агенция „Национална сигурност“ е обвинен в разкриване на информация на частна фирма, което показва пропуски в последващия контрол след напускане на службата [3]. Законът предвижда наказания, но липсата на ясни механизми за проследяване на действията на бившите служители остава слабост, която може да доведе до злоупотреби.

При изпълнение на преките си контролни функции по защита на класифицираната информация служителите на ДАНС извършват ежегодно проверки (планови и инцидентни), при повечето от които са дадени предписания за подобряване на защитата на класифицираната информация, което подсказва, че има пропуски в организациите [4; 5; 6].

Могат да се разгледат основно два аспекта за напускане на службите, при които е възможна злоупотреба с информация, независимо дали е случайно, или умишлено. Първият е свързан с напускане поради пенсионна възраст, независимо дали е по собствено желание на служителя, или във връзка с т.нар. „в интерес на работата“, а вторият е поради причини, породени от различия по отношение на виждания за управление и др. под. И в двата случая обаче става въпрос за служители в работоспособна възраст, което предполага, че те ще продължат да работят в друг сектор, може това да бъде дори частен. Тук е моментът, в който те трябва да бъдат максимално отговорни към закона и лоялни към държавата, за да не си позволят да злоупотребят с информацията, с която разполагат, станала им достояние по време на работа и за която вероятно са се подписали, че ще опазват.

Разбира се, съществува една друга категория служители, които злоупотребяват с достъпна информация с цел получаване на лични облаги. И без да се поставят в тази категория определени служители на службите, най-общо казано, не са малко случаите, които излизат в публичното пространство за злоупотреба с информация именно от тези среди. И тук е мястото да спомена, че казвам това с ясно съзнание и досег до такива ситуации в моята практика.

Ще обърна внимание на още един момент, който често е предизвиквал недоумение не само у мен, но и у доста хора, с които контактувам. Как е възможно бездушие, безучастие и/или неадекватно поведение на служители на службите, когато явно

става въпрос за престъпно деяние? Не е в техните правомощия, не е тяхна работа или още други обяснения, които водят само до едно – бягство от отговорност или явно прикриване на нарушения или още по-зле – на престъпления. Животът на хората не е филм, а реалност, и те очакват да бъдат защитени именно от служителите на службите, най-вече на Министерството на вътрешните работи (МВР) като най-директен представител на властта.

Тук е възможно да бъда упрекната, че смесвам дейността и ролята на институциите, но за тези, които не са разбрали смисъла на казаното по-горе, ще добавя още малко информация.

Държавна агенция разузнаване (ДАР) работи във взаимодействие с другите държавни органи и структури от системата за защита на националната сигурност, които осъществяват дипломатическа, отбранителна, разузнавателна, контраразузнавателна, оперативно-издирвателна, правоохранителна и охранителна дейност [1: 78].

Както по-горе се спомена, устройството, дейностите и функционирането на ДАР, както и статутът на нейните служители се регламентира със Закона за Държавна агенция „Разузнаване“ (ЗДАР). В него са посочени основните функции и дейности и са регламентирани организацията, способите и средствата за изпълнението им. Законът определя институционалното място на разузнаването в системата на изпълнителната власт.

Прегледът на основните закони, които регулират дейността на разузнавателните служби в България, като Закона за Държавна агенция „Разузнаване“, Закона за специалните разузнавателни средства и др., дават пълна яснота за работата с поверителна информация, възникнали нарушения и съответни наказания.

Както се спомена вече, има механизми за контрол и надзор по отношение на дейността на разузнавателните дейности с цел предотвратяване на злоупотреби, и тук главната роля за анализ е отредена на парламента, следват съдебната система и други институции, включително след напускане на службата.

Съществуват правни аспекти и ограничения при работа с поверителна информация, като те включват задължения на служителите да пазят държавна тайна и последиците от нарушаването на тези задължения, включително след напускане на службата. Задължения за конфиденциалност са също част от правните ограничения за служителите относно разкриването на държавни тайни, включително санкции при нарушения след смяна на работното място.

Етически аспекти и предизвикателства

Отвъд правните рамки дейността на разузнавателните служби е пропита с етически дилеми, които стават още по-сложни, когато служители преминават в нови професионални среди. Основният конфликт е между задължението за защита на националните интереси и личните интереси, които могат да възникнат след напускане на службата. В българските служби съществуват кодекси на поведение, които наблягат на лоялността и професионалната честност, но тяхното прилагане след края на службата е трудно измеримо. Обученията по етика, макар и задължителни, често се фокусират върху времето на активна работа, а не върху дългосрочните последици от достъпа до чувствителна информация.

Един от най-сериозните етически проблеми е потенциалното подкопаване на общественото доверие, когато бивши служители използват знанията си за лична или корпоративна облага. Представете си хипотетичен случай, в който бивш анализатор от ДАНС започва работа в частна компания за киберсигурност и използва информация за уязвимости в държавни системи, за да подобри услугите на фирмата. Това не

само нарушава етическите норми, но и поставя под въпрос интегритета на цялата разузнавателна общност. Спокойно може да се постави въпросът за липсата на стриктни етически стандарти след напускане на службите, които да са сред факторите, определящи статута на напускащите. Липсата на такива стандарти е сред факторите, които намаляват доверието на гражданите в институциите за сигурност.

Всъщност от казаното дотук става ясно, че съществува правна рамка, но тъй като липсва контрол по отношение на спазването ѝ, то всичко остава в ръцете на личността на служителя или, казано по друг начин, е въпрос на морални устои, отговорност пред държавата, обществото и самия себе си.

Доколко неспазването на изискванията към определени категории служители е закононарушение или представлява само етическа норма, нека преценят отговорните институции, но за пореден път в годишния доклад на ДАНС за 2020 г. [7] са публикувани нарушения по отношение на защитата на класифицираната информация.

В годишния доклад на ДАНС за 2020 г. [7] се констатира, че Националната система за защита на класифицираната информация остава относително стабилна. Отчита се обаче, че в условия на пандемията от COVID-19 е имало известно затруднение при обмена на класифицирана информация между държавните ведомства поради заболяване и/или карантиниране на конкретни адресати или на служители, отговарящи за тази дейност, съответно липса на механизъм за заместването им в даденото ведомство.

Ето част от констатираните нарушения:

- нарушение с траен характер при прилагане на мерките по персонална сигурност е отказът на лица на изборни длъжности и членове на колективни органи за управление на държавни и частни структури да бъдат проучени и др.;
- нарушенията при мерките за физическа сигурност се дължат основно на неправилно определени зони за сигурност и/или административни зони и достъп до тях в организационните единици и др.;
- установените през 2020 г. нарушения при документалната сигурност продължават да са свързани с дефицити в познаването на нормативната уредба от лицата, ангажирани с обработката, създаването и съхраняването на класифицираната информация [7: 37].

Вероятно е предизвикателство пред определени служители, попадайки в ситуация на конфликти между националната сигурност и личните интереси, особено когато служители напускат службите и преминават в други сектори. Предполагам, това е дилема пред всеки напуснал службите независимо поради какви обстоятелства. Може би съществува и друга дилема или типични етически предизвикателства, пред които са изправени служителите, като балансът между сигурност и граждански свободи, използването на специални разузнавателни средства и др. Тук може да възникне сериозен личен конфликт, не само етически дилеми, при събирането и използването на разузнавателна информация, защото някои случаи могат да бъдат свързани и с нарушения на човешките права от страна на разузнавателните служби.

Действащ от 2014 г. е Етически кодекс за поведение на държавните служители в Министерството на вътрешните работи [8], който регламентира правилата за етично поведение и въвежда етически стандарти при осъществяване на дейността на държавните служители.

От 2020 г. е приет Етически кодекс на военното разузнаване, но за останалите разузнавателни служби препратките са към Закона за Държавна агенция „Разузнаване“.

Имайки предвид това, че една част от информацията за службите не е публична, може да се предполага, че служителите преминават обучения, свързани с прилагане на етически стандарти в българските разузнавателни служби, насочени към предотвратяване на злоупотреби с информация, включително обучения за етично поведение.

Разбира се, съществуват рискове при смяна на работното място, когато бивши служители използват знанията си в нова професионална среда, което може да подкопае общественото доверие. В публичното пространство често се появяват такива случаи и понякога е много сложно да се прецени доколко изнесената информация е вярна, т.е. има злоупотреба, и кога по-скоро целта е уличаване на личността и сваляне на доверие. Със сигурност истината е една, но тя невинаги става достояние на широката общественост.

Всички подобни действия обаче, свързани с използването на поверителна информация в нова професионална среда, могат да подкопаят доверието в службите, особено ако не се появят факти, доказващи или опровергаващи изнесената публично информация.

Можем само да гадаем какво следва с поверителната информация с навлизането в съвременния свят на киберразузнаването. Етическите и правните аспекти са достъпни за по-широка аудитория, докато киберразузнаването може да изисква специализирани познания.

Случаи на преминаване на служители на друго работно място и рискове

Преминаването на служители от разузнавателните служби към други сектори не е необичайно явление в България. Често бивши служители намират работа в частния сектор, особено в сфери, като сигурност, консултантски услуги или дори политика. Този преход крие значителни рискове, тъй като информацията, с която разполагат тези лица, може да бъде използвана за конкурентни предимства или дори за действия срещу националните интереси.

Рисковете включват не само разкриване на държавни тайни, но и използване на специфични познания за методите на работа на службите, което може да улесни частни интереси или дори организираната престъпност. За да се справят с тези заплахи, някои държави, като Великобритания, налагат забрани на бивши служители да заемат определени позиции в продължение на няколко години след напускане на службата [12].

В България подобни мерки са слабо развити, като съществуващите ограничения са предимно формални и не се проследяват ефективно. Разработването на по-строги механизми, като договори за неразкриване с дългосрочен ефект и мониторинг на професионалния път на бившите служители, би могло да намали тези рискове.

Може би по-обстойно изследване на рисковете за националната сигурност, като разкриване на поверителна информация или използването ѝ за лична или корпоративна облага, ще даде по-ясни параметри на това явление.

Възможностите на гражданския контрол върху специалните служби

Основно това са инструментите на парламентарната демокрация – през вота на хората. Тук важното правило е: не могат колеги да контролират колеги. В парламентарните комисии е редно да влизат депутати, отдалечени професионално както от службите за сигурност, така и от службите за охрана. Има криворазбиран професионализъм – компетентни са бивши офицери. Контролът е граждански в най-дълбокия смисъл на понятието. Редът трябва да се проверява от граждани, които имат изходната позиция на цивилни за сектора хора. Трудността тук идва от големите промени в съставите на парламента и необходимостта във всеки нов мандат да се търсят хора, които вече са натрупали опит като депутати в тази област.

Другата форма на контрол е чрез институции, които не са свързани с държавния бюджет – институти и медии. Тук произходът на финансиране на тези контрольори е най-важната тема. Трудно медия – собственост на офшорна фирма, ще направи журналистически разследвания в областта на сектора за сигурност. Причините са ясни. Именно споменатото може да е основа за манипулацията на гражданския контрол – през невежество или чрез защита на организирана престъпност. Може да се проследи и битка между престъпни групировки именно през зависими медии. Това е най-тежкият въпрос от обществена гледна точка.

Културата на възприемане на специалните служби като демократичен инструмент, а не като посткомунистически израстъци, е в пряка зависимост от осветляването им от медиите. Съществува и друг проблем, свързан с лицата, които осъществяват контрола, както в държавните, така и в недържавните институции. И ако при журналисти или изследователи от неправителствения сектор нещата са свързани с техните собственици, ръководители и етическите им рамки, то при народните представители има и друг важен аспект. Една от най-дискутираните теми в европейските институции, занимаващи се с тази тема, е свързана с обема от информация, която могат да получават контролиращите, и съответно какъв обем информация могат да предоставят на медиите. От това пряко зависи и обемът информация, която самите служби ще са склонни да споделят с парламентаристите.

Темата отново е свързана с морални норми. Въпрос е на доверие, че няма да има злоупотреба с тази информация между хората, които контролират. Когато депутатите ползват информация, добита при контрол на специални служби, за трупане на електорални ползи, то не могат да се надяват на прецизност от страна на контролираните.

Ето защо считам, че етическите и правните аспекти на дейността на българското разузнаване и контраразузнаване е тема, която може да се разглежда между актуалност, научна стойност и практическа приложимост.

Заключение

Дейността на българското разузнаване и контраразузнаване е поставена пред сложни правни и етически предизвикателства особено когато става въпрос за преминаването на служители към нови работни места. Правните рамки осигуряват основа за защита на поверителната информация, но липсата на ефективен контрол след напускане на службите оставя вратичка за потенциални злоупотреби. Етическите аспекти подчертават необходимостта от по-сериозен ангажимент към дългосрочна професионална отговорност, докато конкретните случаи показват реалните заплахи за националната сигурност. За да се адресират тези проблеми, е необходимо усилване на санкциите, въвеждане на по-строги етически обучения и сътрудничество с частния сектор за предотвратяване на неправомерно използване на информация. Бъдещи изследвания биха могли да се фокусират върху сравнителен анализ с международни практики, за да се предложат още по-ефективни решения.

По-задълбочено изследване на етическите и правните аспекти на дейността на българското разузнаване и контраразузнаване може да предложи конкретни препоръки за подобряване на законодателството и практиките в областта на разузнаването, което е от полза както за академичната общност, така и за политиците и практиците в сферата на сигурността.

Литература

1. **Велев,** С. и кол. Система за разузнаване. София: Военна академия „Г. С. Раковски“, 2023. ISBN 978-619-7711-26-4.
2. **Годишен** доклад за дейността на Държавна агенция „Национална сигурност“, 2015. [онлайн]. *https://www.dans.bg/bg/activities/reports.*
3. **Годишен** доклад за дейността на Държавна агенция „Национална сигурност“, 2016. [онлайн]. *https://www.dans.bg/bg/activities/reports.*
4. **Годишен** доклад за дейността на Държавна агенция „Национална сигурност“, 2017. [онлайн]. *https://www.dans.bg/bg/activities/reports.*
5. **Годишен** доклад за дейността на Държавна агенция „Национална сигурност“, 2018. [онлайн]. *https://www.dans.bg/bg/activities/reports.*
6. **Годишен** доклад за дейността на Държавна агенция „Национална сигурност“, 2019. [онлайн]. *https://www.dans.bg/bg/activities/reports.*
7. **Годишен** доклад за дейността на Държавна агенция „Национална сигурност“, 2020. [онлайн]. *https://www.dans.bg/bg/activities/reports.*
8. **Етичен** кодекс за поведение на държавните служители в Министерството на вътрешните работи. Обн. *ДВ,* бр. 67, 12.08.2014 г.
9. **Закон** за Държавна агенция „Разузнаване“. Обн. *ДВ,* бр. 79/2007 г.
10. **Закон** за специалните разузнавателни средства. Обн. *ДВ,* бр. 95/1997 г.
11. **Кръстев,** Г. Разузнавателните служби в България – възникване, развитие, перспективи. София: Военно издателство, 2006.
12. **UK** Intelligence Services Act, 1994. [online]. [available 2.04.2025]. *https://www.legislation.gov.uk/ukpga/1994/13/contents*.

HUMAN RESOURCE MANAGEMENT OF UNIFORMED SERVICES IN THE CONTEXT OF LOCAL COMMUNITY SAFETY PERCEPTION

Dariusz Klak, PhD
State University of Applied Sciences in Jarosław, Poland

УПРАВЛЕНИЕ НА ЧОВЕШКИТЕ РЕСУРСИ В УНИФОРМЕНИТЕ СЛУЖБИ В КОНТЕКСТА НА УСЕЩАНЕТО ЗА СИГУРНОСТ В МЕСТНАТА ОБЩНОСТ

д-р Дарюш Клак
Държавна академия за приложни науки в Ярослав, Полша

Abstract: *The aim of this publication is to present the results of research on the sense of security among the residents of the Jarosław County and the assessment of the effectiveness of the actions taken by the uniformed services responsible for maintaining public order. The research, conducted using the diagnostic survey method, revealed a general sense of security among the residents, who appreciated the presence of uniformed services, especially police patrols. Respondents acknowledged that a key factor influencing their sense of security was the frequency of seeing patrols and the familiarity with local services, including the community officer. At the same time, the need for intensifying preventive actions was noted, particularly in improving safety on the streets and in public spaces. The research results suggest that the effectiveness of uniformed services could be further improved with greater visibility and continued educational efforts regarding safety.*

Key words: *human resource management; uniformed services; sense of security; local community; prevention; public safety*

Резюме: *Целта на публикацията е да се представят резултатите от изследвания, свързани с чувството за безопасност у жителите на Ярославския район, както и оценката на ефективността на действията на униформените служби, отговорни за поддържането на обществения ред. Изследванията, проведени чрез метода диагностична анкета, показаха общото чувство за безопасност у жителите, които оцениха присъствието на униформените служби, особено на полицейските патрули. Респондентите посочиха, че важен елемент, влияещ на чувството за безопасност, е честотата на срещите с патрули и познаването на местните служби, включително на участъковия инспектор. В същото време бе отбелязана необходимостта от засилване на превантивните мерки, особено в посока подобряване на безопасността по улиците и в публичните пространства. Резултатите от изследването показват, че ефективността на униформените служби би могла да бъде още по-висока при по-голяма видимост и продължаване на образователните дейности в сферата на безопасността.*

Ключови думи: *управление на човешките ресурси; органи на реда; чувство за безопасност; местна общност; превенция; обществена безопасност*

Introduction

Security is one of the key values that individuals seek to preserve in their daily lives, both on a personal and societal level. This phenomenon is not only the foundation of stability and order but also a crucial factor influencing the civilizational development and functioning of any society. Contemporary understanding of security encompasses not only the military sphere but also various social, economic, and civilizational aspects, including ensuring public order at the local level.

Human resource management in uniformed services, such as the Police, Fire Department, and other agencies responsible for safety, plays a key role in maintaining a sense of security among citizens. Proper deployment of patrols, effective response to threats, and

efficient cooperation with residents are essential to ensuring an adequate level of protection. In the context of the Jarosław County, it is particularly important to understand how the activities of uniformed services affect the perception of security by the local community and which areas require further improvement.

The goal of this publication is to analyze the sense of security among the residents of Jarosław County and to assess the effectiveness of the activities of uniformed services, with particular attention to human resource management within these services. The research aims to determine how the presence of services and their actions influence the sense of security within the local community and what measures could improve the effectiveness of uniformed services in fighting crime and ensuring stability in the region.

Security as a social phenomenon

Security is one of the most important values in human life. It relates to the ability to function within a given society, determining the level of civilizational development and serving as a key factor in the social laws of that society.

Security can be considered from several perspectives: axiological, ontological, and methodological. From an axiological perspective, security is a system of values and judgments. The ontological sense assumes that security is treated as a being. From a methodological point of view, it involves defining the ways to study security. In this view, the standard of security is closely related to the position of humans in the civilized world, and it is also dependent on culture.

Given the diverse interpretations of the phenomenon under analysis, security is linked to political pluralism, freedom of conscience, the principles of the rule of law, property rights, and democracy [2].

The literature on the subject offers numerous attempts to define the concept of security. For example, security is often treated as a state of peace and the absence of threats, sovereignty and integrity, a guarantee of survival, or protection against military and non-military threats [1]. Security is also seen as a process that ensures the functioning of the state and enables its survival [4].

Originally, security was closely related to the military sphere and the preservation of the territorial sovereignty of the state. It was associated with political independence, the survival of the state, or the nation. Today, the concept of security has a much broader scope, as illustrated in *Figure 1.*

As illustrated in the figure, the scope of security is exceptionally broad, which is why it is important to take into account various types of threats. Example categories of threats along with their classification are presented in *Table 1* below.

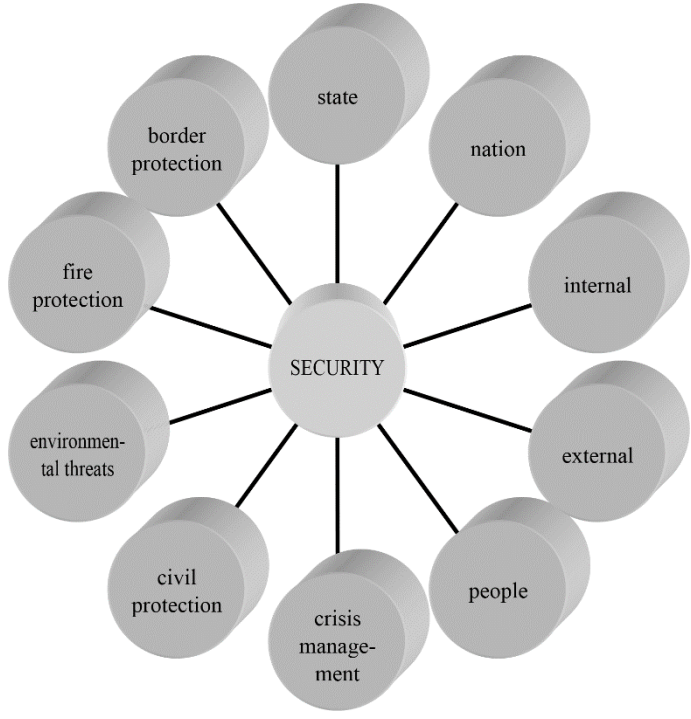
It is important to emphasize that the categories of threats presented in the table are examples and do not exhaust the entire spectrum of issues related to security. In particular, attention should be paid to the dynamic and multidimensional nature of social security, which encompasses not only the stability of social relations but also protection from threats that impact social cohesion, the well-being of citizens, and their sense of security in daily life.

Social security can be considered in three mutually complementary dimensions:

– Social dimension (ensuring citizens have access to basic living conditions, such as healthcare, education, employment, and social security systems);

– Developmental dimension (the opportunities for individual and collective social, economic, and cultural development, contributing to improving quality of life and increasing social capital);

Figure 1. ***Scope of Security***



Source: Zięba, *R. Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych (The Category of Security in the Study of International Relations). Adam Marszałek, Toruń, 2005.*

Table 1. **Typology of Security Threats**

Criteria	Objective
Subject-related	▪ Ecological ▪ Political ▪ Social ▪ Military ▪ Economic
According to the source of threats	▪ Economic ▪ Natural ▪ Educational ▪ Technical ▪ Psychological ▪ Systemic ▪ Cultural ▪ Demographic ▪ Ideological
According to environmental criteria	▪ Scientific-technical ▪ Social

	▪ Economic ▪ Natural ▪ Political
Due to their scope	▪ Global ▪ Regional ▪ Continental ▪ Local
Scale of threats	▪ World level ▪ Individual level ▪ National level ▪ Administrative level ▪ International level
Consequences of threats	▪ Physical ▪ Psychological
Places of threats	▪ Internal ▪ External

Source: *Own elaboration based on:* ***Zboina,*** *J. Bezpieczeństwo na lądzie, morzu i w powietrzu w XXI wieku (Security on Land, Sea, and Air in the 21st Century). CNBOP – PIB, Józefów, 2014;* ***Świętochowski,*** *N. Broń nieśmiercionośna jako środek umacniania bezpieczeństwa państwa (Non-Lethal Weapons as a Tool for Strengthening National Security). FNCE, Poznań, 2018;* ***Otwinowski,*** *W. Wybrane zagrożenia bezpieczeństwa państwa i człowieka (Selected Threats to the Security of the State and the Individual). FNCE, Poznań, 2014.*

– Community dimension (maintaining social cohesion, strengthening interpersonal relationships, and fostering trust and a sense of belonging within local groups and society as a whole).

The state plays a crucial role in shaping security through its structures and institutions responsible for protecting citizens. In particular, services such as the Police, Fire Brigade, and other units and institutions aimed at ensuring public order, the protection of life and property, play a fundamental role in maintaining the security of the local community. The actions of these services, supported by appropriate legal provisions, enable an effective response to threats and prevention, which forms the foundation of stability and citizens' sense of security.

Human resource management of uniformed services in the context of the sense of security of the local community of the Jarosław district

In the context of assessing human resource management in public safety and order services, research was conducted to diagnose the sense of security within the local community of the Jarosław district and evaluate the effectiveness of the uniformed services' actions.

The research questions were formulated as follows:

– Do the residents of the Jarosław district feel safe?

– Are the uniformed services tasked with ensuring security in the Jarosław district effectively performing their duties?

A diagnostic survey method was employed in the study. The request to complete the questionnaire was sent to residents of the Jarosław district via Facebook, providing wide accessibility to the survey and ensuring representative results. For those who expressed interest in participating, the survey questionnaires were sent electronically.

The study group consisted of respondents to whom the surveys were distributed. Out of the sent forms, 120 were returned and formed the basis for further analysis. The collected

responses enabled a detailed analysis of the sense of security among the residents of the Jarosław district and an evaluation of the effectiveness of the uniformed services' actions. (The research was conducted as part of a thesis [3], under the scientific supervision of Dariusz Kłak.)

Among the respondents, 53% stated that they feel safe, while 26% disagreed, and 21% were unsure of their sense of security.

Results regarding particularly dangerous places in the area indicate that 72% of respondents did not identify such places, while 28% considered there to be locations requiring special attention. Nearly half of the respondents (48%) felt safe walking after dark, while 38% expressed a contrary opinion, and 14% had no opinion on the matter.

Regarding the elements influencing the sense of security, 36% of respondents indicated police patrols, while 32% emphasized the importance of knowing the local residents. The frequency of seeing police patrols was also a significant factor – 38% of respondents saw patrols daily, and 33% at least once a week. A police motorized patrol was a source of security for 68% of those surveyed.

When asked about the evaluation of the uniformed services' work in the Jarosław district, 57% of respondents considered it good, and 28% had no opinion.

In terms of knowledge of emergency numbers, as many as 85% of respondents declared that they knew them. 62% of respondents were familiar with their local police officer. When it comes to threats in the immediate surroundings, the most frequently mentioned danger was dangerous drivers (39%), followed by robberies (20%) and fights (13%).

Respondents indicated that most police patrols should be conducted on the streets (41%), followed by the town square (35%) and parks (22%).

The assessment of the safety situation in the district was mainly based on personal observations (48%) and experiences (31%).

Regarding the effectiveness of the uniformed services' actions in fighting crime, 69% of respondents considered them to be effective. The most important safety issues mentioned by residents were drunk drivers (37%), vandalism (17%), and thefts and burglaries (15%).

The conclusions from the conducted research indicate that the residents of the Jarosław district generally feel safe and appreciate the presence of uniformed services. However, there is a need to further strengthen preventive measures, particularly in improving safety on the streets and in public places. It is also important to continue educating residents about safety rules, including knowledge of emergency numbers and the ways to report threats.

The study revealed that the actions of the uniformed services are positively evaluated by most residents, but their effectiveness could be even higher if they were more visible and frequent in places particularly exposed to risks.

Conclusions and recommendations

The conducted research on the sense of security among the local community of the Jarosław district and the effectiveness of law enforcement agencies' actions allowed for drawing important conclusions regarding the management of human resources in these services.

The research results indicate that the majority of residents of the Jarosław district feel safe, and their sense of security is strongly linked to the presence of law enforcement agencies, especially police patrols. Most respondents expressed a positive opinion about the work of law enforcement agencies and assessed their actions as effective in combating crime.

These conclusions suggest a good level of human resources management within the law enforcement services of the Jarosław district, particularly in the area of patrol deployment and the presence of officers in locations that pose potential threats.

However, the research also highlights areas that require improvement. Although the frequency of seeing patrols was relatively high (38% of respondents encountered patrols

daily, and 33% at least once a week), 28% believed that dangerous places existed in their vicinity that needed special attention. This indicates that in certain parts of the district, the number of patrols should be increased, and other forms of prevention should be considered, such as patrolling areas particularly threatened by crime or increasing the presence of law enforcement officers during the evening and night hours when a portion of the residents' sense of security decreases.

In terms of human resources management, important elements also include education and communication with residents. The research shows that 62% of respondents knew their local police officer, which suggests the positive influence of individual relationships between officers and the local community. However, as many as 15% of people did not know the emergency numbers, indicating the need for strengthening educational efforts in this area. Preventive actions, such as informing residents about safety rules and collaborating with law enforcement agencies, can further enhance the sense of security and improve the effectiveness of the services' actions.

Human resources management in law enforcement services should also include regular evaluation of patrol effectiveness and responses to changing threats in a given region. In this context, it is advisable to continue monitoring areas considered dangerous and analyze potential places that may require greater engagement from the services, especially in the case of emerging new threats, such as assaults or aggression on the roads.

In summary, the management of human resources in the law enforcement services of the Jarosław district is positively evaluated, but there is still room for improvement in terms of intensifying preventive actions, improving patrol visibility, particularly in areas deemed dangerous, and increasing educational activities that could raise citizens' awareness and improve their cooperation with law enforcement agencies.

Bibliography

1. **Czupryński,** A. Bezpieczeństwo – teoria, badania, praktyka. (Security – Theory, Research, Practice). Józefów: CNBOP, 2015.
2. **Ferguson,** N. Cywilizacja, Zachód i reszta świata. (Civilization, The West and the Rest). Kraków: Wydawnictwo Literackie, 2013.
3. **Kielar,** J. Poczucie bezpieczeństwa społeczności lokalnej w opinii mieszkańców powiatu jarosławskiego. (Perception of Safety in the Local Community According to the Residents of the Jarosław County). Jarosław: Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. B. Markiewicza w Jarosławiu, 2021.
4. **Marczuk,** K. Trzecia opcja, Gwardie narodowe w wybranych państwach Basenu Morza Śródziemnego. (The Third Option, National Guards in Selected Mediterranean Countries). Warszawa: Fundacja Studiów Międzynarodowych, 2007.
5. **Otwinowski,** W. Wybrane zagrożenia bezpieczeństwa państwa i człowieka. (Selected Threats to the Security of the State and the Individual). Poznań: FNCE, 2014.
6. **Świętochowski,** N. Broń nieśmiercionośna jako środek umacniania bezpieczeństwa państwa. (Non-Lethal Weapons as a Tool for Strengthening National Security). Poznań: FNCE, 2018.
7. **Zboiny,** J. Bezpieczeństwo na lądzie, morzu i w powietrzu w XXI wieku. (Security on Land, Sea, and Air in the 21st Century). Józefów: CNBOP – PIB, 2014.
8. **Zięba,** R. Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych. (The Category of Security in the Study of International Relations). Toruń: Adam Marszałek, 2005.

ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД РАЗУЗНАВАНЕТО И КОНТРАРАЗУЗНАВАНЕТО СРЕД ЕТНИЧЕСКИТЕ И РЕЛИГИОЗНИТЕ ОБЩНОСТИ В БЪЛГАРИЯ

д-р Асен Асенов
Национален съвет за сътрудничество по етническите и интеграционните въпроси към МС

INTELLIGENCE AND COUNTERINTELLIGENCE CHALLENGES AMONG ETHNIC AND RELIGIOUS COMMUNITIES IN BULGARIA

Asen Asenov, PhD
National Council for Cooperation on Ethnic and Integration Issues to the Council of Ministers

Резюме: *Необходимо е да се подчертае, че разузнаването и контраразузнаването сред различните етнически и религиозни групи в страната е тема, която не е разработена. За успешната работа сред тези общности в сферата на сигурността трябва да се подчертае преди всичко тяхната етнопсихология, която не само не се познава, но и често се подценява като маловажен фактор за сигурността на държавата. Актуален въпрос, който в спешен аспект трябва да се разработи, е: в критична ситуация за сигурността на българската държава тези етнически и религиозни групи на какви позиции ще бъдат. Необходим е спешен отговор и дейности по този въпрос.*

Ключови думи: *етнос; религия; сигурност; България; стратегия; разузнаване; контраразузнаване*

Abstract: *It is necessary to emphasize that intelligence and counterintelligence among the various ethnic and religious groups in the country is a topic that has not been developed. For successful work among these communities in the security sphere, it is necessary to emphasize, above all, their ethnopsychology, which is not only unknown, but also often underestimated as an unimportant factor for the security of the state. A topical issue that urgently needs to be developed is: in a critical situation for the security of the Bulgarian state, what positions will these ethnic and religious groups be in. An urgent answer and activities on this issue are needed.*

Key words: *ethnicity; religion; security; Bulgaria; strategy; intelligence; counterintelligence*

Анализът на разузнаването и контраразузнаването във вътрешен план е много деликатна и сложна тема, защото се отнася за дейности, свързани със събирането на информация, анализи и т.н., които се отнасят за населението, живеещо в България. Това положение става още по-сложно и комплексно, когато трябва да се извършва разузнавателна и контраразузнавателна дейност сред различните етнически и религиозни общности, живеещи в България. Тази сложност и трудност идва от това, че определени хора могат да упрекват службите за сигурност в дискриминационно и целенасочено отношение само затова, че те са от малцинствените общности.

Посочените негативни мнения за дейността на разузнаването и контраразузнаването сред различните етнически и религиозни общности в България могат да се тушират и елиминират, когато става въпрос за сигурността на българската държава, в т.ч. и за сигурността на гражданите без значение на етническия им произход и религиозната принадлежност. Необходимо е още веднъж да се подчертае, че сигурността

на всички български граждани трябва да бъде база за обединението на етническите и религиозните общности в страната.

„Без разузнаване не може. Няма уважаваща себе си държава в света, която да се лишава от това мощно средство за придобиване на информация, оказваща съществено влияние върху вземането на решения за развитието на страната и за формирането на нейната вътрешна и външна политика. Умелото използване на тази информация е от изключителна важност за осигуряване на националната сигурност и безопасност на всяка държава“ [1: 9].

Поради различни причини темата за получаването на актуална информация сред етническите общности чрез разузнавателна дейност изобщо не се коментира в българското общество. Каква е причината за това – трудно може да се каже.

В момента чрез различни проучвания и анализи някои изследователи доказват, че няма проблеми сред етническите и религиозните малцинствени общности, които да застрашават сигурността на българската държава. Това не е така и подобни мнения не са полезни, а напротив – вредни за активизирането на дейност в тази насока. Първата задача изисква да се познават не само особеностите на тези общности, но и настоящите процеси, които се развиват сред тях и имат пряко отношение към сигурността на българската държава.

По този въпрос Хр. Тутунаров пише:

„Изготвянето на стратегия за устойчиво развитие и управление на етническите общности и поддържането и развитието на националната идентичност следва да доведе до постигането на задоволителна среда за сигурност и етническа стабилност в България чрез затвърждаване на траен етнически мир в страната, базиран на толерантност, равенство пред закона и запазване на идентичността на етническите общности, но като мегасистема на националната ни идентичност“ [4: 8].

Актуални проблеми сред етническите групи

Ето и няколко актуални проблема сред етническите групи, които са съвременни предизвикателства към службите за разузнаване и контраразузнаване и имат пряка връзка със сигурността на българската държава.

• **Преброяване на населението през 2021 г.**

Според това преброяване населението на България е 6 519 789 души, от които:

– българи – 5 664 624 души, т.е. 84,8 %;

– турци – 588 318 души, т.е. 8,8 %;

– роми – 377 506 души, т.е. 4,9 %;

– не посочили етническа принадлежност – 405 961 души;

– отказали да участват в преброяването – 371 536 души.

Според преброяването 777 497 души не се самоопределят в етническо отношение. Това е реален проблем за сигурността на българската държава, защото тези хора могат да променят устойчивата етническа структура на държавата. Службите за сигурност трябва да съберат допълнителна информация по този въпрос, за да се види какви са причините и в близките 5 – 6 години към коя общност ще се интегрират – българската, турската или нова етническа общност.

Съвременната турска общност в България

По въпроса за турската общност трябва да се посочи, че сред нея има сериозни динамични процеси, които невинаги се регистрират:

– капсулирането на тази общност продължава да се задълбочава, което е много сериозен проблем за българското общество;

– необходимо е да се подчертае, че тази общност до 1989 г. имаше нагласи и отношения, които след 90-те години на XX век се промениха, и то в негативен план;

– в момента обръщението към тях може да бъде само „турци“, но не и „български турци“, което те не приемат, като по този въпрос има няколко телевизионни предавания в Турция;

– при самоопределението си те не само подчертават, че са турци, но добавят, че са „османски турци“, което до скоро време го нямаше;

– използват исляма като основен елемент на етническата си идентичност.

Процесите сред помаците в България

Допреди 10 години тази общност се делеше на две – българи и турци. Новото сред тях е, че има вече и трети момент в тяхната етническа идентичност – помашката общност, като в момента в Гърция има създаден научен център „Помак“.

Ислямът, разузнаването и контраразузнаването в България

Изследователите на исляма в България много често изучават теологичните измерения на тази религия, без да анализират неговото обществено, етническо, религиозно и друго значение.

„Наш приоритет бяха институциите и религиозните общности извън територията на България, стремящи се към проникване и провеждане на религиозната пропаганда вътре в страната, ислямските фундаменталистки организации, изграждащи канали за насилствено налагане на исляма в България. Някои от каналите работеха така перфектно, че зад тях прозираше умелата направляваща ръка на професионалистите от тайните служби“ – пише А. Кременлиев [2: 191].

Реалните проблеми, които имат пряко отношение към сигурността на българската държава на базата на исляма, са следните:

• **Стълбовете на исляма**

Според теологията си ислямът има пет стълба: 1) шахада – засвидетелстване на единобожието и на пророчествата на Пророка Мухаммад; 2) салат – неотстъпно спазване на петте канонични молитви през деня; 3) зекят – задължителна милостиня; 4) постенето през месец Рамадан; и 5) хадж – задължението всеки мюсюлманин поне веднъж в живота си да посети светите за мюсюлманите места Мека и Медина.

През последните години се правят сериозни опити без канонично основание да се въведе шести стълб – джихад.

„Джихад“ произлиза от арабска дума със значение „стремя се“, „полагам усилие“, „боря се“. Точното значение зависи от контекста“ [3: 100].

• **Ролята на салафитската секта в България**

През последните 5 – 6 години представители на салафитите се опитват да навлизат в структурите на ислямското вероизповедание и постепенно да ги изместят. Тази секта в редица държави в Европа е забранена по следните причини: 1) отричат светските закони и конституциите и признават само шариата; 2) не признават съвременния ислям, а само „салаф“, в смисъл на „благочестивите предци“, особено първите три мюсюлмански поколения, които според традицията са водили праведен живот съобразно нормите на традиционния ислям.

• **Ислямът и етническата идентичност**

Въпросът за ролята на исляма като важен етнообразуващ елемент за принадлежност не е нов, а съществува от много години.

Особеностите на „турския ислям“ са в това, че той има преди всичко задълбочаване на етническата идентичност чрез:

„Всеки мюсюлманин е турчин, всеки турчин е мюсюлманин“.

В същото време трябва да се посочи, че „арабският ислям“ има други цели: задълбочаване на религиозното съзнание и поведение без значение на етническия произход, създаване на голяма „световна умма“, т.е. световна мюсюлманска общност, която работи системно за разширяване и задълбочаване на ислямското влияние.

„Последвалите събития след демократичните промени влошиха етническата карта на България. Решенията се взимаха прибързано и под уличен натиск. Новоизлюпените демократи се заиграха с етническата карта, без да мислят за последствията. България се нуждае от нова концепция по националния въпрос, приета и провеждана с консенсус от всички отговорни политически сили, така както от векове практикуват нашите съседи на Балканите“ – пише Атанас Кременлиев [2: 239].

Този цитат най-добре очертава проблемите в сферата на сигурността и дейността на разузнавателните и контраразузнавателните органи в България през последните 35 години.

Предложения

1. Разработване на нова Национална стратегия на България с раздел „Мерки и дейности сред етническите и религиозните общности в България“.
2. Създаване към службите за разузнаване и контраразузнаване на сектор „Анализи на съвременните етнически и религиозни процеси и националната сигурност“.
3. Назначаване в службите за сигурност на хора от различните етнически групи, които отговарят на необходимите изисквания.
4. Изучаване на етнопсихологията в университетите във връзка с националната сигурност и тероризма.
5. Откриване към университетите на магистърска програма „Етнорелигиозните процеси и националната сигурност на България“.
6. Служителите в службите за сигурност да бъдат обучавани в АМВР за по-успешна работа с етническите и религиозните групи, като се обърне внимание на терминологията, етнопсихологията, факторите за формиране на етническа идентичност, исляма в България и в Европа, изграждане нова концепция за антитеористична дейност и др.

Заключение

Темата за разузнавателната и контраразузнавателната дейност в аспекта на новите етнически и религиозни процеси не е разработена не само в научно отношение, но и в нейното практическо приложение, защото не се познават и много често се подценяват тези проблеми.

Трябва да се посочи, че промените в Европа и отражението им върху България правят темата за етническите и религиозните общности и сигурността на държавата много актуална. Необходимо е да се посочи, че България е много уязвима от гледна точка на сигурността и териториалната цялост на базата на етносите и религиите. На този етап в България няма научни разработки, които да очертаят един много актуален проблем за сигурността: в критичен за България момент какво ще е поведението на етническите и религиозните групи, на чия страна ще застанат.

Много е важно службите за сигурност с помощта на експерти и специалисти да отговорят на тези актуални въпроси, докато все още има време. Този подход трябва

да се определи като успешна дейност в сферата на разузнаването и контраразузнаването, което ще гарантира националната сигурност и териториалната цялост на Република България.

Литература

1. **Благоев,** П. Загадката на българското разузнаване. София: Хайни, 2009.
2. **Кременлиев,** А. Из лабиринтите на българското разузнаване. София: Св. Климент Охридски, 2011.
3. **Оксфордски** речник на исляма. София: Рива, 2007.
4. **Тутунаров,** Хр. Етнически общности и национална сигурност в България. София: Изток – Запад, 2015.

НАЦИОНАЛНАТА ГВАРДИЯ НА БЪЛГАРИЯ

гл. ас. д-р Иван Винаров
Университет за национално и световно стопанство – София

THE NATIONAL GUARD OF BULGARIA

Chief Ass. Ivan Vinarov, PhD
University of National and World Economy – Sofia

Резюме: *В настоящия доклад анализираме проблема за Българската национална гвардия в две направления. От една страна, през годините, непосредствено предшестващи присъединяването на страната ни към НАТО, бяха лансирани инициативи за създаване на национална гвардия под формата на паравоенна единица, т.е. на „резервна“ армия по западен (американски и британски) модел. Опитите за създаване на „четвърта въоръжена сила“, или „гвардия за териториални действия“ (на базата на публично-частно партньорство), обаче така и не се осъществиха. От друга страна, България има свой създаден гвардейски корпус от традиционен тип. Той е създаден от княз Александър I непосредствено след възкачването му на престола (1879 г.). С течение на времето, освен церемониалната си функция, той проявява героизъм и в реална бойна ситуация – в конфликта със Сърбия през 1885 г., по време на войните за национално обединение (1912 – 1918 г.) и Втората световна война (1940 – 1944 г.). След началото на промените Националната гвардейска част се превръща в един от символите на българската държавност (наред със знамето, герба, химна и др.). Структурата ѝ включва двата гвардейски батальона, представителния духов оркестър и ансамбъла на Въоръжените сили, както и „гвардейските училищни дружини“.*

Ключови думи: *Александровска звезда; гвардейска униформа; Национална гвардейска част; паравоенно формирование; символ на българската държавност*

Abstract: *In this report we analyze the problem of the National Guard of Bulgaria in two directions. On the one hand, in the years immediately preceding our country's accession to NATO, initiatives were launched to create a National Guard in the form of paramilitary formation, i.e. „reserve“ army of the Western (American and English) model. However, attempts to create a „fourth armed force“ or „guard for territorial action“ (based on public-private partnership) never materialized. On the other hand, Bulgaria has its own established Guard Corps of a traditional type. It was created by Prince Alexander I immediately after his accession to the throne (1879). Over time, in addition to ceremonial function, it also demonstrated heroism in a real combat situation – in the conflict with Serbia in 1885, during the wars of national unification (1912 – 1918) and the Second World War (1940 – 1944). After the beginning of the changes, the National Guard Unit became one of the symbols of Bulgarian statehood (along with the flag, coat of arms, anthem, ect.). Its structure included the two Guard Battalions, the representative brass hand and the ensemble of the Armed Forces, as well as the „Guard Student Units“.*

Key words: *Alexander Star; Guards uniform; National Guard Unit; paramilitary formation; symbol of Bulgarian statehood*

Увод

В настоящия доклад анализираме проблема за Националната гвардия на България в две направления. От една страна, през годините преди присъединяването на нашата страна към НАТО са лансирани инициативите за създаване на национална гвардия под формата на паравоенно формирование, т.е. „резервна“ армия по западен (американски и английски) образец. Но опитите за създаване на „четвърта въоръжена

сила“, или „гвардия за териториално действие“ (на базата на публично-частно партньорство), така и не се реализират. От друга страна, България има свой утвърден гвардейски корпус от традиционен тип. Той е създаден от княз Александър I непосредствено след неговото изкачване на престола (1879). С течение на времето той, освен церемониалните функции, проявява и героизъм в реална бойна обстановка – в конфликта със Сърбия през 1885 г., по време на войните за национално обединение (1912 – 1918 г.) и Втората световна война (1940 – 1944 г.). След началото на промените Националната гвардейска част се превръща в един от символите на българската държавност (заедно със знамето, герба, химна и т.н.). В нейната структура се включват двата гвардейски батальона, представителният духов оркестър и ансамбълът на Въоръжените сили, както и „гвардейските ученически отряди“.

Национална гвардия – паравоенна („резервна“) армия по западен образец

През годините идеята за изграждане на национална гвардия е лансирана неедноктратно в обществения дневен ред. През февруари 2002 г. началникът на Генералния щаб ген. Никола Колев оповестява, че до една година ще бъде изградена национална гвардия с до 15 хил. служещи. Идеята цели решаването на два належащи проблема: от една страна, нуждата от паравоенно формирование, което да бъде използвано при нужда от помощ вследствие на бедствия, мащабни аварии и т.н.; от друга страна, по този начин се осигурява работа на планирания за съкращаване военен персонал – през първите години на XXI в. няма характерното за днес недокомплектоване на въоръжените сили и много офицери, вместо да преминават в резерв, могат да бъдат преназначавани в гвардията (като техните звания се запазват и при необходимост е възможно по всяко време да бъдат върнати на предишната им длъжност) [14].

Три години по-късно, вече в условията на членство на България в НАТО, е формулирана идеята за изграждане на национална гвардия по американски образец, която да бъде на двойно гражданско-военно подчинение, с мирно- и военновременни задачи. Сп. Спиридонов: *„Образно казано, ставаше дума за една резерва армия, която да осигури надеждна защита на населението не само при мирновременни кризи“.* Предвижда се още във времето, в което гвардейците изпълняват задачи, да получават възнаграждение (под формата на заплата) в пълен размер. Те ще са подчинени на вицепремиера, министъра на държавната администрация или на този, който отговаря за бедствията и авариите. Финансирането ще се осигурява от държавния бюджет по две линии, което води до двойно подчинение на гвардията – на военните и на областните управители [12].

Междувременно през 2004 г. експерти стигат до заключението, че не е добре да се създава „паралелна“ армия – своеобразна *„четвърта въоръжена сила“,* която да е на пряко подчинение на държавния глава като върховен главнокомандващ на въоръжените сили. Ген. Аню Ангелов (по-късно военен министър) дава превес на доброволческия тип отряди, които да са на разположение на областните управители и кметовете. Изграждането на териториален резерв като структура към Централното военно окръжие по места така и не се реализира [12].

С премахването на задължителната военна служба на 31.12.2007 г. в политическия елит избледнява желанието за създаване на гвардейски корпус от американски или британски тип. Въпреки това българските военни не изоставят идеята. През април 2016 г. създателят и председател на Съюза на българските командоси проф. Юлий Абаджиев заявява, че *„една добре организирана структура от 50 – 70 хил. души за адекватна реакция са безценен ресурс“* [16]. И допълва: *„Готови сме да направим*

Национална гвардия на базата на публично-частно партньорство. Националната гвардия е за териториални действия, не за военни. Тя ще бъде локализирана в съответните области и трябва да бъде въоръжена с техника за действие в кризисни ситуации" [4].

В Програмата за развитие на отбранителните способности на Въоръжените сили на Република България, 2032, приета на 1.02.2021 г., е записано: *„Въоръжените сили поддържат способности за превенция, ранно предупреждение и неутрализиране на потенциални рискове и заплахи за националната сигурност (…) оказват помощ (…) за провеждане на спасителни, евакуационни и неотложни аварийно-възстановителни работи за овладяване и/или преодоляване на последствия при бедствия…"* [11]. Казано по друг начин, нужда от подобен тип квазивоенно формирование в действителност има, но е възприет подход с неговите функции да бъде натоварена професионалната армия, която всъщност е в ситуация на тревожно голям кадрови недостиг (в т.ч. в резерва).

Националната гвардейска част

Всяка една държава, която е създала и поддържа собствени въоръжени сили, въвежда в тяхната структура формирование, което наред с другите свои задължения (произтичащи най-често от законодателството, свързано с официалния държавен протокол) изпълнява и представителни (парадно-церемониални) функции. В България тази задача е поверена на Националната гвардейска част (НГЧ) [7]. Тя е приемник на личната гвардия на княз Александър I Български (Батенберг), създадена през 1879 г. Първият официален ескорт на младия монарх е осъществен на 12 юли с.г., поради което тази дата е официалният празник на НГЧ. Първоначално частта е изградена като лична свита на княза и неговото семейство, която придружава официалните гости при посещение на нашата столица. През десетилетията гвардията се променя от княжески конвой в ескадрон, полк, а през 1942 г. придобива статут на дивизион. Днешната функция на НГЧ е отдаването на военни почести и представителен духов оркестър за участие в правителствени и официални церемонии. Гвардейската униформа е създадена през 1883 г. и включва елементи, характерни за ранната българска национална символика. През последния век и половина незаменими остават два елемента – орловото перо на гвардейския калпак и Александровската звезда (която е символ и на българския царски орден „Св. Александър"). През 2002 г. за кадровите военнослужещи в НГЧ е изработен нагръдник, който е съчетание между Александровската звезда и новата национална символика [10].

Призванието на НГЧ е да участва във формирането и поддържането на патриотичната мотивация и националния дух на обществото, както и утвърждаването на българската идентичност и държавност. Гвардията е част от културната политика на Министерството на отбраната в областта на военно-патриотичната, културно-възпитателната и концертната дейност. Девизът на НГЧ е: ***„За честта и славата на Родината!"*** [17].

Основните гвардейски ценности са [17]:

* ***вярност:*** да се спазва Конституцията на Република България, като се изпълняват безпрекословно законите, уставите и заповедите на командирите и се съхраняват утвърдените духовни ценности;

* ***храброст:*** безстрашно да се защитават целостта и независимостта на страната и интересите на народа;

* ***дълг и чест:*** да се приема заповяданата мисия и нейното изпълнение като лична отговорност, без да се нарушават общоприетите правни и морални норми;

* ***безкористна служба:*** да се поставят успехът и благото на Родината, народа и останалите военнослужещи над собственото благополучие и интереси;

* ***достойнство:*** безупречно да се изпълняват воинските задължения и да се служи за пример в обществото.

История на Националната гвардейска част

С встъпването на престола на Александър I през лятото на 1879 г. става необходимо изграждането на специална военна част с охранителни и представителни (церемониални) функции. На 12 юли с.г. Софийска № 1 конска сотня осъществява първия официален ескорт на младия български княз, като е предвождана от личния флаг на Батенберг. С Указ № 28 от 30.08.1879 г. Първа конна сотня е определена за Собствен конвой на княза. През десетилетията тя се разраства от 150 на 600 души състав през 40-те години на XX в. Специалното отношение на всички държавници към нея води до приоритетното ѝ снабдяване с най-модерното снаряжение, въоръжение и най-добрите породисти коне. По този начин до 1944 г. гвардията се утвърждава като елитна бойна войскова единица – тя е в основата на създаването на високоподготвени офицери, които достигат до висши позиции в йерархията на българската армия. Сред нейните главнокомандващи са някои от най-утвърдените имена в историята на родното военно изкуство: Петър Марков, Христо Петрунов, Иван Колев, Генко Мархолев, Александър Кисьов, Любомир Босилков, Константин Соларов, Александър Танев и др. От средите на гвардейското офицерство се избират хората от свитата на монарха. Флигел-адютантът на княза (царя) задължително е гвардеец. Той именно е човекът, който придружава непосредствено българския монарх при пътуванията в чужбина. Сред задълженията на гвардията е и охраната на държавни, военни и стопански обекти, които попадат под юрисдикцията на Софийския гарнизон. **Сред тях най-важният е почетният караул на парадния вход на двореца, неизменно изпълняван от 1882 г. с часови, винаги облечени в парадна гвардейска униформа** [9].

Като елитна част гвардейците са първи при връчването на бойните знамена – те са единствената войскова единица с право да носи както личния флаг на българския владетел, така и официалното бойно знаме на армията. По тази причина на 30.08.1881 г., след връчването на първите официални бойни знамена в нашата история, гвардията и останалите войскови части изпълняват церемониален марш пред княз Александър I [9]. Грижата на първия български монарх за новосъздадената гвардия остава като един от положителните елементи на неговото властване. Според Дияна Костова (от Националния военноисторически музей) тази част *„е вплела в себе си националната символика. Заслуга за нейното създаване има и самият княз, който лично участва в изработката на първите рисунки на модели и в подбора на сукното за униформата“* [7]. Заедно с първия командир на гвардейското формирование – поручик Ал. Мосолов, правят графиките на основата на униформата на конницата (най-авторитетния род войска по това време). На основата на хусарската униформа те обогатяват проектомодела с български традиционни национални елементи. В крайна сметка се получава красиво парадно военно облекло, което е посрещнато с одобрение от всички [8].

Първото извънцеремониално действие на гвардията е през септември 1885 г., когато заради провъзгласяването на Съединението заедно с монарха пристига в Пловдив. Пресичайки Балкана през връх Св. Никола, гвардейците ритуално свалят своите шапки. **Защото именно те са първите, които прекрачват несъществуващата вече граница между „двете Българии“.** Именно на гвардейците се пада задачата да охраняват границата заради евентуален отговор от страна на Османската империя. По време на Сръбско-българската война участват в боевете при Драгоман и Пирот. **Датата 15.11.1885 г. завинаги ще остане в историята на българската гвардия –**

именно тогава нашата конница се изправя в победоносна битка срещу сръбския еквивалент. След подписването на примирието Лейбескадронът е посрещнат триумфално в София, а на Александровския площад в негова чест е проведен невиждан дотогава на Балканите военен парад [10].

Безгранична храброст Лейбгвардеският конен полк проявява и през войните за национално обединение. **През януари 1916 г. е включен в състава на Конната дивизия с командир ген. Иван Колев и се сражава в битката за Добруджа.** Геройството и храбростта, което проява българската армия за свободата на поробения от румънците три години по-рано Североизток, няма как да бъдат описани в един кратък доклад. През ноември 1838 г. Гвардейският полк участва в официалната делегация, водена от военния министър ген. Теодоси Даскалов, която присъства на погребалната церемония на Кемал Ататюрк. През последните дни на септември и първите на октомври 1940 г. полкът е част от Трета българска армия начело с ген. Стефан Тошев. Тя реализира практически освобождението на Добруджа след подписването на 7 септември с.г. на Крайовската спогодба между правителствата на България и Румъния. През април 1941 г. е сред първите, които са посрещнати като освободители на Македония в началото на процеса по администриране на областта от българска страна. А през 1944 г. конният дивизион участва в заключителния етап на войната срещу нацистка Германия [6]. Броят на загиналите гвардейци през периода от 1885 до 1945 г. е седемдесет и двама.

Националната гвардейска част днес

През 2001 г. Националната гвардейска част е утвърдена като представително военно формирование на българската армия и един от символите на държавността заедно с националното знаме, химн, герб, държавен печат и столицата – град София [10]. В нейната структура се включват: 1) войскови единици за отдаване на военни почести – *Първи гвардейски батальон* (представително подразделение за участие в протоколни мероприятия и церемонии) и *Втори смесен гвардейски батальон* (провежда 21 артилерийски салюта при посещение на държавни глави и 20 салюта при честване на националния празник 3 март и пр.); 2) *Гвардейски представителен духов оркестър* – създаденият през 1951 г. (под името Централен духов оркестър на БНА) първокласен художествено-изпълнителски колектив е с основни заслуги за естетическото и музикалното възпитание на българските воини. В изпълненията му се съчетават произведения в широк музикален диапазон – от фолклорни ритми, през военни маршове, до класика, естрада, джаз и рок. През последните години реализира съвместни проекти с Детския радиохор и с популярните изпълнители Еделина Кънева, Орлин Горанов, Маргарита Хранова, Орлин Павлов и Васил Петров. Участва и на международни фестивали на военните духови оркестри (в Германия, Франция, Швейцария, Белгия, Турция, Дания, Русия, Израел, Румъния, Босна и Херцеговина и т.н.); и 3) *Представителен ансамбъл на Въоръжените сили* – основен културен и творчески институт на българската армия с безспорен авторитет в културния живот на нашата страна. Почти половината от изнасяните от него представления са пред гражданската публика в цяла България. Част от неговия състав са били творци от ранга на Филип Кутев, Никола Гюзелев, Кичка Бодурова, Христо Кидиков, Нели Рангелова, Георги Христов, Михаил Белчев, Симеон Щерев и др. [15].

НГЧ участва в мероприятия, в които нашата страна се представя по официален път от президента на републиката, председателя на Народното събрание, министър-председателя, министъра на отбраната или началника на Генералния щаб на Българската армия. НГЧ има свое знаме, печат и отличителен знак [1]. Гвардията придобива

престижна публичност, подобна по стойност на връчваните от президента на републиката ордени и медали, става символ на държавническата традиция в смисъла, който се влага в националния и официалните празници, паметниците на културата (в т.ч. старите български столици, сградите – символи на българската държавност и църковна независимост), националната валута – лева, и т.н. [3].

Гвардейците от почетния караул покоряват ежедневно погледите на жителите и гостите на столицата София. Те са на предните редици по време на представителни и официални церемонии, протоколни мероприятия и военни ритуали с държавен ранг и от национално значение. **От своя страна гвардейската униформа също е емблема на българската държавност и е видим израз на военните ни традиции и доблест.** Тя вплита в себе си националната символика и е доказателство за приемствеността (континуитета) между поколенията. Въпреки че е почти изцяло запазена в първоначалния си вид отпреди век и половина, съвременната гвардейска униформа се отличава с новаторство и блясък, присъщи на българския воин. Според Д. Арнаудов от щаба на НГЧ службата в нея *„изисква висока духовна нагласа, висока мотивация и не само това – изисква и носенето на специална униформа, която не само да бъде символ на самата армия, но и своеобразен елемент на държавността“* [8].

Една от най-важните представителни задачи на НГЧ е смяната на почетния гвардейски караул на парадния вход на Президентството. Първата подобна церемония е осъществена на 5.11.2003 г. Целта на събитието е утвърждаване на нов ритуал, свързан със съхраняването и развитието на традициите, заложени в нашето славно минало. Смяната на почетния караул се провежда точно в 12:00 ч. на следните официални празници: 3 март – Ден на Освобождението от турско иго (Национален празник на Република България); 6 май – Ден на храбростта и празник на Българската армия; 24 май – Ден на българската просвета и култура и на славянската писменост; 2 юни – Ден на Ботев и загиналите за свободата на България; 12 юли – Празник на националната гвардейска част; 22 септември – Ден на независимостта на България; 1 ноември – Ден на народните будители; както и всяка първа сряда в месеца без декември, януари и февруари.

Наред със задачите, произтичащи от Закона за държавния протокол и Устава на Въоръжените сили на Република България, НГЧ има роля и при създаването на т.нар. „гвардейски ученически отряди“. Първият от тях е създаден в Кърджали през 2006 г., а към ден днешен подобни съществуват в още 16 български града (в т.ч. Бургас, Велико Търново, Габрово, Гоце Делчев, Плевен, Русе, Смолян и пр.). По думите на майор Николай Стоянов – началник на щаба на Първи гвардейски батальон: *„За тези отряди трябва да кажем, че повлияват изключително благотворно върху възпитанието, което започва от ранна възраст. Целта е опазването на историята ни и възкресяването на традициите, както и възпитанието на любов и чувство на принадлежност към родината у младото поколение“* [7].

В края на 2005 г. с подкрепата на Националния дарителски фонд „13 века България“ е осветен Паметникът на гвардейците жертви пред олтара на Отечеството 1885 – 1945 г. Инициативата е израз на дълбокото преклонение пред подвизите на загиналите воини от гвардията. Целта е техните имена никога да не бъдат забравени. Мемориалът съчетава изображение на Александровската звезда и орлово перо – символ на гордия и непобедим български дух, които са отляти от бронз. От двете страни на перото се издигат бетонни колони, към които са прикрепени гранитни плочи с имената на 7-ната гвардейци, изгубили живота си в името на борбата за национално обединение на България. Под Александровската звезда е изписан девизът на НГЧ, а на гърба на паметника е прикрепен лавров венец от бронз [6].

* * *

Националната гвардия – церемониален „посланик“ на България пред света (Вместо заключение)

През последните години на Националната гвардейска част е оказана голямата чест да представя България на най-високо церемониално равнище. На 14.07.2022 г. военно формирование на НГЧ е част от традиционния парад по повод на Деня на Бастилията – Националния празник на Франция. В него участие взимат 6300 души, от които 5000 – в пешия марш. В парада се включват и 64 самолета, един дрон, 25 хеликоптера, 200 коня и 181 моторизирани превозни средства. **Българските гвардейци с националния флаг на Република България водят на първата линия пешия марш на Шан-з-Елизе и представят Родината пред Европа и света по най-достойния начин.** Зад нашето формирование маршируват представители на още осем държави – Естония, Литва, Латвия, Полша, Чехия, Словакия, Унгария и Румъния. Накрая след тях преминават френските военни [14].

На 14 юни 2023 г. представители на НГЧ на България гостуват във Ватикана на Папската швейцарска гвардия. Нейният командир полк. Кристиян Граф приема командира на българската гвардия полк. Иван Иванов, придружаван от десет гвардейци, членове на 18 младежки гвардейски отряда, директори на училища, университетски преподаватели и студенти от различни висши училища. Поводът за срещата е обмяна на опит в службата на гвардейските части, който се предава от дългогодишната история на двете гвардии към съвременните предизвикателства [2].

Литература

1. **Андреева,** Кремена. История и традиция: тържествената смяна на почетния гвардейски караул. – В: *DarikNews,* 3.03.2025 г. [онлайн]. [достъпен 10.05.2025]. *https://dariknews.bg/novini/bylgariia/istoriia-i-tradiciia-tyrzhestvenata-smiana-na-pochetniia-gvardejski-karaul-video-2377024*.
2. **Ватикана** – Националната гвардейска част на България – Папска швейцарска гвардия. – В: *Българска телеграфна агенция.* [онлайн]. [достъпен 12.05.2025]. *https://www.bta.bg/bg/galleries/221153.*
3. **Винаров,** Иван. Политическата криза в България 2021 – 2023. Избори, изборни системи и структура на парламентарното управление. Пловдив: ВУСИ, 2023.
4. **Да** има ли Национална гвардия? – В: *Българска национална телевизия,* 19.04.2016 г. [достъпен 3.04.2025]. *https://bnt.bg/bg/a/da-ima-li-natsionalna-gvardiya*.
5. **Жеков,** Венцислав. Празничен концерт за Гергьовден. – В: *Army Media,* 13.05.2023 г. [онлайн]. [достъпен 10.05.2025]. *https://armymedia.bg/2023/05/13/празничен-концерт-за-гергьовден/*.
6. **История.** – В: *Национална гвардейска част.* [онлайн]. [достъпен 8.04.2025]. *https://www.guards-bg.com/история/*.
7. **Колев,** Йоан. Гвардейската униформа – един от символите на храбростта на българския войник. – В: *Българско национално радио,* 6.05.2023 г. [онлайн]. [достъпен 10.05.2025]. *https://bnr.bg/radiobulgaria/post/101818423/gvardeiskata-uniforma-edin-ot-simvolite-na-hrabrostta-na-balgarskia-voinik*.
8. **Любопитно** за гвардейската униформа: история и символика. Миланова, Йоана. (Ред.). – В: *DarikNews,* 6.05.2017 г. [онлайн]. [достъпен 10.05.2025]. *https://dariknews.bg/novini/bylgariia/liubopitno-za-gvardejskata-uniforma-istoriia-i-simvolika-snimki-2021854*.
9. **Миланова,** Ивана. 12 юли – Празник на националната гвардейска част. – В: *ГЛАС Пресс,* 12.07.2017 г. [онлайн]. [достъпен 10.05.2025]. *https://glaspress.rs/12-юли-празник-на-националната-гвардей/*.
10. **Национална** гвардейска част. – В: *Президент на Република България,* 30.12.2012 г. [онлайн]. [достъпен 7.04.2025]. *https://m.president.bg/bg/cat75/Nacionalna-gvardeiska-chast.*

11. **Програма** за развитие на отбранителните способности на въоръжените сили на Република България, 2032. София: Министерски съвет, 2021.
12. **С** тържествен военен парад с участието и на български гвардейци в Париж бе отбелязан френският национален празник. – В: *Army Media,* 14.07.2022 г. [онлайн]. [достъпен 12.05.2025]. *https://armymedia.bg/2022/07/14/франция-отбелязва-националния-си-пра-2/*.
13. **Славова,** Ваня. 84 години от връщането на Южна Добруджа. – В: *Българско национално радио,* 7.09.2024 г. [онлайн]. [достъпен 8.04.2025]. *https://bnr.bg/varna/post/102042739*.
14. **Спиридонов,** С. Националната гвардия – екзотика или необходимост. – В: *Информационен център на Министерството на отбраната,* 16.10.2022 г. [онлайн]. [достъпен 3.04.2025]. *https://armymedia.bg/2022/10/16/националната-гвардия-екзотика-или-н/*.
15. **Структура.** – В: *Национална гвардейска част.* [онлайн]. [достъпен 10.05.2025]. *https://www.guards-bg.com/структура/*.
16. **Торошанова,** Анелия. България има нужда от Националната гвардия. – В: *Българско национално радио,* 16.10.2022 г. [достъпен 7.04.2025]. *https://bnr.bg/post/100554522*.
17. **National** guards unit. – В: *Национална гвардейска част.* [онлайн]. [достъпен 8.04.2025]. *https://www.guards-bg.com*.

РИСК И СИГУРНОСТ. РИСКЪТ В СТРАТЕГИИТЕ ЗА НАЦИОНАЛНА СИГУРНОСТ В БЪЛГАРИЯ

гл. ас. д-р Рада Смедовска-Тонева
Институт по философия и социология към БАН

RISK AND SECURITY. THE CONCEPT OF RISK IN THE NATIONAL SECURITY STRATEGIES IN BULGARIA

Chief Ass. Rada Smedovska-Toneva, PhD
Institute of philosophy and sociology, BAC

Резюме: *С развитието на рисковата социология понятието „риск“ постепенно придобива автономност и набира сила в политически и институционален дискурс. В съвременното общество политиките за сигурност от реактивни се стремят да бъдат проактивни, следвайки максимата, че повече си струва да действаме днес, защото възможността за катастрофа в бъдеще е толкова пагубна, че не можем да рискуваме, като бездействаме. Текстът проследява терминологичното развитие на стратегическите документи в България в сферата на националната сигурност по отношение на понятието „риск“, кога се появява, в какъв контекст и до каква степен се използва при формулирането на политиките за сигурност.*
Ключови думи: *риск; заплаха; сигурност; оценка на риска; управление на риска*

Abstract: *With the development of risk sociology, the concept of risk is gradually gaining autonomy and strength in political and institutional discourse. In contemporary society, security policies have moved from being reactive to being proactive, following the maxim that it is more worthwhile to act today because the possibility of catastrophe in the future is so disastrous that we cannot risk by inaction. The text traces the terminological development of the strategic documents in the field of national security with regard to the notion of „risk“, when it appeared, in what context and to what extent it is used in the formulation of security policies in Bulgaria.*
Key words: *risk; threat; security; risk assessment; risk management*

Увод

В несигурния свят, в който живеем, все по-често започваме да чуваме за различни по характер рискове, с които разнообразни сфери от нашия живот се сблъскват – екологически, здравни, финансови, икономически, геополитически, социетални и т.н. „Рискът“ е сравнително ново понятие, което постепенно заема едно от централните места в политиките за сигурност в редица държави. Политическият, и най-вече институционалният език му отделят специално внимание и ориентират говоренето си около него, поради което и употребата му в стратегическите документи за сигурност на държавите става все по-интензивна. В началото на 90-те години присъствието му е по-скоро спорадично, но към края на миналия век рискът се утвърждава като един от основните концепти в областта на сигурността.

„Рискът“ е понятие, което се свързва с дадена ситуация, с дадено явление, изначално обгърнато в несигурност и неяснота, което обаче институциите трябва да превърнат в измеримо и предотвратимо. Макар и да има допирни точки с други, сходни на него понятия, като „заплаха“, „опасност“, „предизвикателство“, „несигурност“ и пр., рискът е самостоятелна категория. За разлика от тях той изисква и по-различна

политика, характеризираща се с по-гъвкави елементи и отчитане на редица неопределености и фактори [6: 20].

В много държави политиките за сигурност са подчинени именно на риска. Великобритания и Холандия са едни от примерите в тази област, защото техните стратегически документи за национална сигурност показват, че смисълът на политиките не е толкова в гарантирането на сигурността, а в идентифицирането, анализа, оценката, въздействието и мониторинга на риска, т.е. тези елементи, които в днешно време определят процеса на т.нар. „управление на риска“ [7: 537]. Този текст беше провокиран от идеята да се проследи до каква степен България следва тази тенденция и дали рисковото мислене е навлязло в концепциите и стратегиите за национална сигурност, тъй като това са основополагащи документи и задават тона и ориентацията на политиките са сигурност. Анализът се фокусира върху понятийната и смисловата употреба, т.е. кога се появява, как еволюира през годините и до каква степен служи за основа на ориентирането на политиките за сигурност.

Секюритизация или рискификация

Настоящият текст няма за цел да проследи научния дебат относно понятията „сигурност“, „заплаха“, „риск“, тяхното значение и различни смислови трактовки, защото това само по себе си е обект на самостоятелен и задълбочен анализ. Тук само ще кажа, че и заплахата, и рискът може да бъде основен елемент от генералната концептуализация на сигурността. В този контекст едно от теченията, които следва да се споменат, е т.нар. „Копенхагенска школа“, която развива концепцията за „секюритизация“, анализирайки процеса, при който властите дефинират определено явление като екзистенциална заплаха и легитимират използването на извънредни мерки, за да му се противопоставят. Тази концепция оспорва традиционното разбиране за сигурността като за нещо обективно дадено и разгръща идеята, според която конкретни проблеми се конструират като въпроси на спешна и екзистенциална заплаха, което води до потенциално прекомерни реакции, излизащи извън ограниченията и контрола на правната и политическата система [11]. Тя създава теоретична рамка за критичен анализ на политическата динамика, която улеснява нарастването на извънредните мерки, предприемани от различните държави. Тези извънредни мерки са свързани с конкретни действия, политики или средства, които властта използва за справяне със съответните заплахи, които поради своя спешен и застрашителен характер не могат да бъдат преодолени, следвайки нормалните правила и процедури.

Други изследователи предлагат различен подход, акцентирайки върху идеята за риска. Те смятат, че е по-удачно рискът да се превърне в централно понятие в сферата на сигурността, заместващи заплахата [12: 235 – 258]. Според техните виждания рискът изисква ново схващане за сигурността, тъй като за разлика от заплахата, която е по-ясно обособена и осезаема, рискът е навсякъде, но съществува като някаква вероятност. Тоест редица аспекти в обществото могат да се дефинират и посочат като риск [12: 235 – 258], но това не означава, че те ще се реализират. Едни от първите поддръжници на тази идея са Улрих Бек и Антъни Гидънс, които смятат, че рискът е перманентна характеристика на съвременното общество и в повечето случаи е непредсказуем и непредвидим [2]. Той би преобърнал мисленето относно сигурността, защото в този случай властите ще насочват вниманието си към потенциалните рискове, а не толкова към съществуващите заплахи. В този контекст изследователите започват да говорят за навлизането на т.нар. „рискификация“, т.е. за наличието на социален процес, при който даден политически въпрос се конструира през призмата на риска [7]. Именно елементът на вероятност е този, около който ще се фокусират и

политиките – те няма да са реактивни и насочени към защитата от определени заплахи, а ще са превантивни и обърнати към редуциране на вероятността рискът да настъпи или в случай, че настъпи, – към намаляване на нивата на щетите, които би нанесъл. Политиките ще следват максимата, че е по-добре да се действа отрано, за да се избегне настъпването на бъдеща криза, която би изисквала налагането на спешни и извънредни мерки. Или, иначе казано, традиционната политика в сферата на сигурността, която предполага предприемането на спешни и извънредни мерки, ще бъде изместена от друг вид политика – политика на постоянство и дългосрочно планиране. Тя ще се фокусира върху различните по характер рискове и нейната основна цел няма да се състои в тяхното елиминиране, тъй като те не могат да бъдат изкоренени, а в ефективното им управление.

За рисковото мислене в сферата на националната сигурност в България

Целта на една стратегия за национална сигурност е да се определят всички заплахи и рискове, които могат да засегнат живота на нацията по отношение на защитата на населението, целостта на територията и устойчивостта на институциите в държавата. Всички публични политики трябва да бъдат насочени и да допринасят за гарантирането на националната сигурност. Това е концепцията, която допринася за по-колективното разбиране на заплахите и рисковете, засягащи живота на една нация. Дълбоките взаимозависимости на отворения свят, процесите на глобализация я изправят пред редица предизвикателства, което потвърждава не само смисъла ѝ, но и значимостта на начина, по който тя подхожда към дефинирането на заплахите и рисковете по отношение на въпросите на сигурността и суверенитета на държавата. Това е така, защото рано или късно всичко опира до стратегическите документи за национална сигурност и институционалните държавни политики следва да се ръководят от тях.

Първият стратегически документ след промените в България през 1989 г. е приет сравнително късно – Концепцията за национална сигурност е от април 1998 г. В нея се отбелязва задълбочаването на икономическите и социалните различия на континента, а заедно с тях и появата на „нова несигурност и нови рискове“, без обаче да се посочват какви са те. Отчита се, че „Балканите са зона на конфликти и напрежение в Европа, което създава сериозни рискове за националната сигурност на България“. Въз основа на концепцията и правомощията си Министерският съвет ежегодно трябва с доклад пред Народното събрание да „посочва рисковете за страната и да дава оценка на степента на защита на националните интереси“. От своя страна Съветът по сигурността „обобщава, анализира и прави изводи от цялата текуща информация за рисковете пред националната сигурност и дава професионална оценка и прогноза за динамиката на опасностите“.

Понятийно концепцията е най-слабо развита по темата за рисковете. В нея като че ли понятията се смесват и не се прави разграничение между рискове, заплахи и опасности. Това до голяма степен е разбираемо и е валидно не само за българските стратегически документи. Подобна е ситуацията и в други държави, което се дължи на факта, че езикът на рисковете е все още прохождащ и тепърва навлиза в разработването на концептуални документи в сферата на сигурността. „Заплахата“ е доминантното понятие, липсва ясно разграничение между риск и заплаха и те в повечето случаи се използват като взаимнозаменяеми.

В следващите две стратегии – от 2011 и 2018 г., се наблюдава развитие. Чисто терминологично употребата на самото понятие „риск“ зачестява. Обособява се отделна глава „Рискове и заплахи“, но те все още вървят ръка за ръка. В Стратегията от 2011 г. терминът „риск“ се използва 32 пъти, от които 15 пъти „риск“ и „заплаха“ вървят заедно, а „заплаха“ се среща 29 пъти, от които 14 пъти самостоятелно [3: 252]. На всичките места и трите понятия – „риск“, „заплаха“, „опасност“, са взаимнозаменяеми. Ако все пак обаче се опитаме да направим съдържателно разграничение, то бихме могли тематично да отличим сферите, в които се използват тези понятия.

а) От известното към заплахата

За заплаха се говори в случаите, когато става дума за тероризъм, регионални конфликти, икономически, финансови и демографски кризи. Описаните по-горе явления са по-скоро традиционни проблеми и заплахи, т.е. те съществуват през годините и се проявяват по сравнително познат начин. Разбира се, при преценката относно традиционния или нетрадиционния характер следва да се отчитат съвременният политически контекст и начинът, по който заплахата се проявява спрямо него [7: 39]. Но в общи линии това са проблеми, чиито негативни последици вече са започнали да се усещат и материализират. Поради тази причина и институционалният отговор се състои в предприемането на редица реактивни мерки, чрез които се цели неутрализирането им и справянето с тях до някаква определена степен. В този смисъл за тях важи повече и традиционната политика за сигурност, според която мерките са по-скоро реактивни.

Липсата на ясно понятийно разграничение в езика на сигурността неминуемо рефлектира върху съдържанието и посланията на стратегическите документи. Пример за това е заплахата от тероризъм и радикализация, която е допълнително развита и в Стратегията за противодействие на радикализацията и тероризма, приета през 2015 г. в рамките на политиките за сигурност. Малко след атаките от септември 2001 в САЩ някои изследователи посочват, че този вид тероризъм „е пример за нова асиметрична стратегическа реалност, която е много по-успешно разбрана през понятието „рисково общество“, отколкото от традиционното схващане за тероризма [13: 285 – 395]. Впоследствие и други автори насочват вниманието към идеята, че тероризмът следва да се разглежда в контекста на рисковата парадигма [10: 89 – 115]. Въпреки че в общите стратегии в България тези явления попадат в категорията на заплахите, в тази изрично е посочено, че се набляга върху превенцията, затова и една от целите ѝ се състои в разработване на механизми и индикатори за идентифициране, наблюдение и оценка на рисковете от радикализация на определени сегменти в обществото. Подобно на стратегиите за сигурност, и тук терминологично рискове и заплахи вървят ръка за ръка. В стратегията са идентифицирани традиционните рискове и заплахи от радикализация и тероризъм, но почти не се обръща внимание на тяхното управление. Въпреки акцента върху превенцията в целия текст на стратегията превенция и противодействие в повечето случаи се употребяват заедно.

Киберпрестъпността също е в графата „Заплаха“ в общата Стратегия за национална сигурност от 2018 г. През 2016 г. е приета и Национална стратегия за киберсигурност „Киберустойчива България 2020“, която се окачествява като един от най-прогресивно написаните стратегически документи. В нея се наблюдава понятиен преход от киберсигурност към киберустройчивост. Направено е и разграничение между двете понятия: „заплаха“ – факт или събитие с потенциал, който може да нанесе сериозни вреди на дейността на организации, активи, хора или даже на държавата чрез неоторизиран достъп, разрушаване, разкриване и промяна на данни и/или отказ от услуги. Рискът е определен като потенциална възможност дадена заплаха да бъде реализирана, като се експлоатира уязвимостта на активите, за да се

причини вреда. Предвиждат се периодичен преглед и оценка на рисковете и заплахите, както и подобряване на координираните мерки за защита. Оценката на нивото на киберсигурността се извършва на базата на стандартизирани методи и класификация на рисковете. Въпреки това обаче рискове и заплахи вървят ръка за ръка и се използват като взаимнозаменяеми.

б) От неизвестното към риска

С навлизането на идеята за рисковото общество се смята за логично, ако не и неизбежно, да се появяват качествено нов вид проблеми – такива, които пораждат рискове и които представляват риск. Важното за тези рискови проблеми е, че те трябва да бъдат атакувани изпреварващо и енергично, за да не излязат извън контрол, което да увеличи общата несигурност [7: 40]. Бъдещите потенциални предизвикателства за сигурността, като климатичните промени, пандемиите, миграцията, демографските проблеми обикновено минават през идеята за риск. Подобна е тенденцията и в Стратегиите за национална сигурност от 2011 и 2018 г. Те описват с рисковата терминология миграционния натиск, засилването на влиянието на радикални движения в непосредствена близост до Европа, ескалацията на въоръжените конфликти в световен мащаб, повишаваща риска от реализиране на незаконни оръжейни доставки, нарастващата в световен мащаб опасност от разпространяване на оръжия за масово унищожаване. Отчита се и увеличаването на риска от продължаващите опити на отделни държави да придобиват и развиват ядрен и ракетен потенциал за военни цели.

За разлика от 2011 г., когато демографската криза минава под шапката на заплахата, през 2018 г. тя е окачествена като риск. Анализът на данните за основните здравно-демографски показатели показва, че в момента страната ни е изправена пред съществени рискове за националната сигурност, свързани с високо ниво на обща и преждевременна смъртност, високо ниво на майчина и детска смъртност, високо ниво на степен на увреждане и трайна неработоспособност и ниска продължителност на живота в години, както и в години на добро здраве.

Рискът се среща по-отчетливо и когато става дума за екологическа сигурност, за зависимост на държавите от жизненоважни ресурси (енергийни, водни, суровинни и хранителни). Всъщност един от секторите, в които рисковата парадигма има най-явно отражение, е именно екологическата сигурност. Тя е обект на отделен документ – Национална стратегия за намаляване на риска от бедствия (2018 – 2030) [5]. Специална секция „Управление на риска“ набляга на необходимостта от прилагането на политики и стратегии за намаляване на риска от бедствия. Превенцията е описана като наличие на нормативни изисквания, организационни и физически мерки, насочени към избягване или намаляване на негативните последици от бедствия. Тази сфера като че ли най-успешно се вписва в лексиката на риска в контекста на съвременното рисково общество. Тя създава усещане, че политиките за сигурност започват постепенно да се обвързват с рисковите проблеми. Това обаче до голяма степен се дължи на характера на бедствените явления, които изискват разнообразни и изпреварващи действия.

Рисковата парадигма съдържа няколко предимства. Първо, езикът на риска, за разлика от този на заплахата, предоставя по-широк инструментариум от гледна точка на възможните действия. Второ, в случай на заплаха институциите разполагат със значително по-малко време за противодействие, защото нейната степен на непосредствена деструктивност е много по-висока. Поради това тя изисква бърз и конкретен отговор, понякога дори и въвеждане на извънредни мерки. Трето, заплахата е с по-ниска степен на определеност за разлика от риска, чиято степен на вероятност да настъпи подлежи на преценка и измерване. В този смисъл и мерките, които той налага, влизат в сферата на „по-меките“, дългосрочни и устойчиви политики. Четвърто, лексиката на

риска пресъздава оптимистичната гледна точка и вдъхва повече спокойствие в усещането за сигурност. Създава се чувството, че всички работим заедно, за да изградим по-сигурна среда за всички нас. Това е в духа на изследователите (global risk management school), според които рискът налага възприемането на политика, обърната към управление и справяне, а не толкова към защита и елиминиране. Тоест няма да се стремим да изкореним съответния риск, а действията ще са насочени към намаляване на неговото въздействие и последици, в случай че той се реализира. Акцентът е поставен много повече върху превантивните мерки и проактивните действия.

В несигурните времена, в които живеем, в които не всички рискове биха могли да бъдат елиминирани, ключът към успешните действия е устойчивостта – способността държавата да се възстанови, ако рискът се материализира. Общото усещане в българските стратегически документи е, че действията все още са защитноориентирани и са насочени към противодействие на отделните заплахи и рискове. Мисленето в много голяма степен реактивно. Непрестанното смесване на понятията и паралелното им използване свидетелстват за формалната, и по-скоро механична употреба на понятието „риск“. То просто присъства в синхрон с общата международна тенденция, свързана с навлизането му в речника на сигурността. Използването му в стратегическите документи обаче не води до съществена трансформация на концептуализацията за сигурността. Ако имахме подобна промяна, текстовете щяха да са подчинени на две отчетливо различни логики. От една страна, щяхме да имаме заплахите, които граматически и речниково се свързват с конфронтация, агресия, враг, елиминиране и защита. Затова те изискват бърз и конкретен отговор. От друга страна, е рискът, обвързан с несигурност, бъдещи предизвикателства, възможности, потенция, управление, смекчаване, устойчивост, измерване, превенция и пр. Вследствие на това рискът подлежи на оценка, а вероятността за неговата реализация – на измерване. Действието на тези различни езикови конфигурации провокира и наличието на два различни подхода по отношение на сигурността – можем да противодействаме на тероризма като действителна заплаха (например преследване на ръководителите на международните терористични групировки), но в същото това време можем да действаме превантивно по отношение на рисковете чрез предотвратяване на радикализацията.

Заключение

Рисковете, рисковата проблематика и работата с рисковите сфери са една от фундаменталните линии, които трябва да следват политиките за сигурност във всяка държава. Необходимо е властите и институциите да насочват вниманието си към въпроси, свързани с това как се идентифицират рискове в средата, кои са основните рискове в краткосрочен и дългосрочен план, какви ресурси трябва да се отделят и как се приоритизират рисковите сектори. Пандемията от 2020 г. ни показа значението на механизмите за управление на кризата с Covid-19 и необходимостта от редукция на рисковете от разпространение на епидемията. Ситуацията беше валидна не само за България, но и за много голяма част от развитите държави в света.

В съвременното общество схващанията за сигурността са много повече обвързани с идеята за управление на риска, отколкото с постигането на съвършена сигурност [14: 40 – 45]. Поради тази причина и понятието трябва да е самостоятелно и да не се обърква и слива с други, като „заплаха“, „опасност“, „несигурност“, „уязвимост“ и пр. Разбирането за риска се развива паралелно с развитието на обществото. Затова и понятието „риск“ се смята за ключово, защото в него се оглежда обществото и по него можем да разберем повече неща за самото общество. Процесът на разбиране е

пряко свързан с процеса на управление, т.е., колкото по-добре разбираме обществото, толкова по-успешно ще допринесем за неговото управление [7: 203].

Промяната в концептуализацията на сигурността изисква не само преосмисляне на лексиката и логиката на стратегическите текстове, но и по-активна и подробна регламентация на работата с рискове от страна на институциите за сигурност. Вниманието трябва да е насочено много повече към анализ, оценка, идентифициране и наблюдение на рисковете, което автоматично ще засили и проактивното действие, т.е. ранното сигнализиране и намаляването на възможните рискове. Работата по редукция на рисковете изисква тяхната ясна и системна приоритизация, което би трябвало да бъде формулирано на концептуално ниво – нещо, което към момента е сериозен дефицит в стратегическите документи в България.

Литература

1. **Актуализирана** стратегия за национална сигурност, 2018 г. Приета с Решение на НС от 14.03.2018 г. Обн. *ДВ,* бр. 26 от 23.03.2018 г.
2. **Бек,** У. Рисковото общество. София: Критика и хуманизъм, 2013.
3. **Иванова,** Ел. Терминът „риск“ и „заплаха“ в Стратегията за национална сигурност на Република България. – В: *Научни* трудове на Русенския университет, том 51, серия 7, 2012, с. 252.
4. **Концепция** за национална сигурност, 1998 г. Приета с Решение на НС от 16.04.1998 г. [онлайн]. *https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=655.*
5. **Национална** стратегия за намаляване на риска от бедствия, 2018 – 2030 г. [онлайн]. *https://www.strategy.bg/strategicdocuments/View.aspx?lang=bg-BG&Id=1279.*
6. **Попов,** Ст. Риск. Концептуална рамка. София: Нов български университет, 2022.
7. **Слатински,** Н. Рискът: новото име на сигурността. София: Изток – Запад, 2019.
8. **Стратегия** за национална сигурност, 2011 г. Приета с Решение на НС от 8.03.2011 г. [онлайн]. *https://www.strategy.bg/StrategicDocuments/View.aspx?Id=671.*
9. **Стратегия** за противодействие на радикализацията и тероризма (2015 – 2020 г.). Приета с Решение № 1039 на МС от 30.12.2015 г. [онлайн]. *https://www.strategy.bg/strategicdocuments/View.aspx?lang=bg-BG&Id=979.*
10. **Aradau** and Van Munster. Governing terrorism through risk: Taking precautions, (un)knowing the future. – In: *European* Journal of International Relations, 13, 1, 2007, pp. 89-115.
11. **Buzan,** B, O. Waever, J. de Wilde. Security: A new framework for analysis. London: Lynne Rienner Publishers, 1998.
12. **Corry,** O. Securitisation and Riskification: Second-order security and the politics of climate change. – In: *Millenium* Journal of International Studies, 40, 2, pp. 235-258, 2012. [online]. DOI: 10.1177/0305829811419444.
13. **Rasmussen,** M. V. Reflexive security: NATO and international risk society. – In: *Millenium* Journal of International Studies, 2001, 30 (2): 285-395. [online]. DOI: 10.1177/03058298010300020901.
14. **Wæver,** O. Security: A Conceptual History for International Relations, Version 3.1. – In: *Annual* meeting of the International Studies Association, New Orleans, 24-27 March 2002, pp. 40-45.

ТЪМНИТЕ СТРАНИ НА „ПУБЛИЧНАТА ДИПЛОМАЦИЯ“

д-р Петър Атанасов
Пловдивски университет „Паисий Хилендарски“

THE DARK SIDES OF „PUBLIC DIPLOMACY“

Petar Atanasov, PhD
Plovdiv University „Paisii Hilendarski“

Резюме: *Докладът изследва възможните връзки между меката сила, публичната дипломация и дейности, като шпионаж, психологически операции и намеса във вътрешните работи на различни държави.*
Ключови думи: *мека сила; публична дипломация; шпионаж; психологически операции*

Abstract: *The report explores the possible connections between soft power, public diplomacy, and activities such as espionage, psychological operations, and interference in the internal affairs of various countries.*
Key words: *soft power; public diplomacy; espionage; psychological operations*

В своята книга „Флорентински истории“ Николо Макиавели включва един интересен разговор, в който заключението може да се разглежда като прекрасна илюстрация на теорията за меката сила и свързаните с нея дейности:

„Какво от наша гледна точка е подозрително в поведението на Козимо? Със своите средства той помага на всички: и на частните лица, и на държавата, и на флорентинците, и на кондотиерите. Той ходатайства пред магистратите за всеки гражданин и благодарение на всеобщото предразположение към него може да издигне този или онзи от своите привърженици до най-почитаните длъжности. Излиза, че трябва да бъде осъден на изгнание за това, че е състрадателен, услужлив, щедър и обичан от всички. Кажи ми кой е този закон, който забранява, осъжда, порицава състраданието, великодушието и любовта към ближния? Разбира се, към такива средства прибягват обикновено онези, които се стремят към върховната власт, обаче не всички са съгласни с това...“ [2: 223].

В съвремието съществува една по същество полезна дейност, занимаваща се с взаимно разбиране, хуманитарна подкрепа, образователни дейности, научни изследвания и други полезни за човечеството и в частност за някои държави дейности и в повечето случаи стремяща се да излъчва „състрадание, великодушие и любов към ближния“, дейности, които нито един закон не забранява, не осъжда и не порицава. Тази дейност е получила названието „публична дипломация“. Освен откритата си и приветлива страна, публичната дипломация има и своите сенчести страни.

Съвременната публична дипломация е законен наследник и развитие на пропагандните методи и методите на психологическата война и психологическите операции, прилагани от враждуващите държави в Първата и Втората световна война. Особено развитие тя получава през годините на Студената война, когато се и оформят академичните постановки на „меката сила“ и се формулира терминът „публична дипломация“ като нещо разграничено от пропагандата. Мека сила и публична дипломация са чисто академични формулировки, приети в момента за нещо напълно нормално във външната политика, но нямат никаква международна правна обвързаност,

за разлика от конвенционалната дипломация. Липсата на правна обвързаност и международноправни ограничения създава изключително широко поле за творчески изяви в тази област. Така например:

„Прието е да се говори за жанрове на публичната дипломация. В тази употреба понятието „публична дипломация „е родово понятие, под което се подвеждат профилирани видове дипломация. Такива например са културната дипломация, бизнес дипломацията, научната дипломация, хуманитарната дипломация, екологическата дипломация, спортната дипломация, църковната дипломация, парламентарната дипломация, диаспората дипломация, дигиталната дипломация. В съвременността съществува тенденция тези видове дипломация да се множат и да се разграничават“ [4: 50 – 51].

В момента публичната дипломация може да се разбира като взаимодействие с чуждестранната експертна общност и гражданското общество, насочено към защита на стратегическите приоритети на дадена държава. Публичната дипломация е близка до хуманитарното сътрудничество и е един от елементите на хуманитарната политика, която включва и подпомагане на международното развитие (следконфликтно развитие, реакция при кризи). Целта на публичната дипломация е да формира механизми за диалог и да създаде привлекателен образ на държавата, която инициира публичната дипломация.

„Очерняне“ на имиджа на друга държава с помощта на инструменти, като пропаганда, контрапропаганда и дезинформация, не се смята за елемент на публичната дипломация, но и не съществува изрична юридически оформена забрана.

През втората половина на XX в. в Съединените щати терминът „публична дипломация“ се разглежда като заместител на съветския термин „пропаганда“. По време на Студената война тези понятия имаха почти синонимни значения.

Постепенно публичната дипломация се отдалечи от пропагандата, но сега има тенденция да се върне към корените си. Напоследък в почти всички държави по света се наблюдава „милитаризация на публичната дипломация“ [1].

Политологът Джоузеф Най-младши формулира термина „мека сила“, определяйки го като способността на страната да влияе на другите, без да прибягва до принудителен натиск. На практика този процес включва държавите да проектират своите ценности, идеали и култура през границите, за да насърчат добрата воля и да укрепят партньорствата.

Меката сила обикновено произхожда извън правителството, на места, като училища, религиозни институции и благотворителни групи. Също така се формира чрез музика, спорт, медии и големи индустрии, като Силиконовата долина и Холивуд.

Но това не означава, че правителствата отсъстват от култивирането и използването на мека сила.

Така например по време на Студената война САЩ и Съветският съюз използват тази форма на влияние като ненасилствен метод за популяризиране на своите културни, икономически и политически ценности. Съответните прояви на мека сила се използват, за да подкопават противоположните идеологии.

Съветските лидери например полагат големи усилия, за да изградят последователи на комунизма в чужбина, като инвестират сериозно в пропагандни кампании и социалистически младежки движения [7].

Компонентите на публичната дипломация са:

а) изслушване (основата на всяка ефективна публична дипломация);

б) застъпничество;

в) културна дипломация;

г) обмен; и

д) международно излъчване.

Но също така се идентифицира:

е) психологическата война като паралелна дейност, която споделя някои ключови характеристики с публичната дипломация, но която трябва да се управлява отвъд твърда защитна стена.

Слушането е най-важно за управлението на международната среда чрез събиране и съпоставяне на данни за аудиторията и нейните мнения в чужбина и използване на тези данни за съответно пренасочване на обществената политика или по-широк подход на публична дипломация.

Въпреки че систематичните оценки на чуждото мнение са модерни, настроението на съседа е характерно за докладите на разузнаването, откакто съществуват шпиони [8].

Психологическата война е извън повечето концептуализации на публичната дипломация, а също и извън повечето бюрокрации на публичната дипломация. Дори е противоречиво включването на тази област в анализ на публичната дипломация. Тук обаче ще го разглеждаме наред с приетите подобласти на публичната дипломация като паралелна дейност. В международния контекст на информацията психологическата война може да се дефинира като използване на комуникация от актьор за постигане на цел по време на война, обикновено чрез комуникация с обществеността на врага. Типичните цели са да се пречупи волята на врага за съпротива или да се улесни предаването или несъгласието в редиците на врага.

Психологическата война е планирано тактическо използване на пропаганда, заплахи и други небойни техники по време на войни, заплахи от война или периоди на геополитически вълнения за подвеждане, сплашване, деморализиране или по друг начин повлияване на мисленето или поведението на врага.

Докато всички нации го използват, Централното разузнавателно управление на САЩ (ЦРУ) изброява тактическите цели на психологическата война (PSYWAR) или психологическите операции (PSYOP) като:

– помощ за преодоляване на волята на врага да се бие;

– поддържане на морала и спечелване на съюза на приятелски групи в държави, окупирани от врага;

– влияние върху морала и отношението на хората в приятелски и неутрални към Съединените щати държави.

За да постигнат целите си, планиращите кампании за психологическа война първо се опитват да придобият пълно познание за вярванията, харесванията, нехаресванията, силните страни, слабите страни и уязвимостите на целевата група. Според ЦРУ знанието какво мотивира целта е ключът към успешната PSYOP.

Война на ума

Като несмъртоносно усилие за улавяне на „сърцата и умовете“ психологическата война обикновено използва пропаганда, за да повлияе на ценностите, вярванията, емоциите, разсъжденията, мотивите или поведението на своите цели. Целите на такива пропагандни кампании могат да включват правителства, политически организации, групи за застъпничество, военен персонал и цивилни лица [9].

Ето и някои определения на институционално ниво:

„Публичната дипломация – откритият обмен на идеи и информация – е присъща характеристика на демократичните общества. Глобалната му мисия е централна за (...) външната политика. И остава незаменим за (…) [националните] интереси, идеали и лидерска роля в света“ (Из Доклад на Консултативната комисия на САЩ по публична дипломация, 1991 г.).

Цел: Постигане на национални цели, без да се прибягва до сила, или да действа като мултипликатор на силата, в случай че е необходима сила.

Цел: „Засилване на сигурността на САЩ, укрепване на икономическия просперитет на Америка и насърчаване на демокрацията в чужбина“.

При реорганизацията на Държавния департамент на 1.10.1999 г. Евелин Либерман става първият заместник-секретар по публична дипломация и обществени въпроси. Както отбелязва тя в изслушването си за потвърждение, „[П]убличната дипломация, практикувана в хармония с традиционната дипломация, ще ни позволи да прокараме нашите интереси, да защитим нашата сигурност и да продължим да осигуряваме моралната основа за нашето лидерство в света“ [10].

Тук всъщност е интересен въпросът какви средства ще бъдат използвани за целта. И този въпрос е решен в книгата на Сол Алински „Rules For Radicals“. Той казва, че политическите реалисти трябва да виждат света такъв, какъвто е: арена на политиката на властта, движена предимно от възприеманите непосредствени лични интереси, където моралът е риторична обосновка за целесъобразни действия и лични интереси.

По този начин основният въпрос: „Оправдава ли целта средствата?“, е определен като безсмислен. Истинският и единствен въпрос относно етиката на средствата и целите е формулиран като: „Оправдава ли тази конкретна цел това конкретно средство?“ [5].

Както вече беше отбелязано, между публичната дипломация, меката сила, шпионажа и психологическата война има тясно преплитане както на ниво определения, така и на ниво практика.

Инструментариумът и целите всъщност са взаимнозаменяеми, универсални и допълващи се. Ето два типични примера:

Руската публична дипломация има своите корени в Съветския съюз. От гледна точка на идеологическата работа през втората половина на XX в. СССР понякога се оказва в по-силна позиция от САЩ. Така СССР има цяла система, изградена на високо ниво: от институтите на Академията на науките до такива организации, като Съюза на съветските дружества за приятелство и културни връзки с чужбина.

Руската публична дипломация започва да се възражда през 2000 – 2010 г., когато са създадени редица специализирани структури: Фондацията за подкрепа на публичната дипломация на името на А. М. Горчаков; Съветът по външна и отбранителна политика; клуб „Валдай“; Фондацията за подкрепа и защита на правата на сънародниците, живеещи в чужбина; Националният изследователски институт за развитие на комуникациите (НИИРК); Мемориален фонд „Андрей Карлов“; Асоциацията за изследване на външната политика на името на А. А. Громико; Руската хуманитарна мисия „Творческа дипломация“; Интеграционният клуб към председателя на Съвета на Федерацията; Националният комитет за изследвания на БРИКС; международни проекти на Федералната агенция по въпросите на младежта („Росмолодёж“); Руският младежки съюз; Асоциацията на обществените сдружения; Националният съвет на младежките и детските асоциации на Русия и др.

Проблемът с публичната дипломация обаче е следният: резултатите от усилията, положени за провеждането на събитието, са видими едва след 10 години. Поради тази причина серия кръгли маси на руски и китайски учени в областта на техническите науки изглежда по-ефективен инструмент на публичната дипломация в случая [1].

А ето и някои „недовършени работи“, засягащи пряко нашия регион, и в частност България.

Според Елена Пономарьова и Мирослав Младенович най-показателният пример за недопустимостта на пренебрегването на публичната дипломация е политическата и хуманитарната катастрофа в руско-украинските отношения. Фактът, че почти

80 % от украинското население според оценката на председателя на парламента на Новоросия О. А. Царев в момента има предпазливо и негативно отношение към Русия, е резултат не само от киевската пропагандна машина, но и от недостатъци от руската страна. Освен това в случая става дума не само за кризата след Майдана, но и за всички постсъветски десетилетия.

От 1991 г. степента на руското хуманитарно влияние върху украинското общество не просто е намаляла. Има бавно, но съзнателно изместване на ценностите – общи за нашите държави и народи. Резултатът от тази политика, на която Русия не отговори правилно, е появата преди всичко сред младите хора на невероятно агресивни русофобски настроения. Това състояние на нещата се влошава от фактическото оттегляне на Русия от хуманитарното пространство на съседната държава: 87 % от студентите от Украйна участват в западни програми, но практически никой не знае нищо за руските програми.

Но не само съвременна Украйна служи като упрек за недостатъците на Русия в областта на публичната дипломация. Всъщност Русия загуби дори такъв исторически и културно близък регион, като Балканите. В случая става дума преди всичко за православни държави. Пряко доказателство за това е по-специално ежегодното нарастване на броя на сърбите, които гледат положително на присъединяването на страната не само към ЕС, но и към НАТО. Освен това Черна гора, която Александър III нарече (след руската армия и флот) „най-надеждния исторически съюзник на Русия“, тъй като не е член на ЕС, на 11.04.2014 г. се присъедини към антируските санкции и по-късно стана 29-ата държава – член на НАТО [3].

Очевидно, трябва да се работи и да се работи...

Следните държавни и недържавни институции участват в системата на публичната дипломация на САЩ: Държавният департамент, Министерството на отбраната, Американската агенция за международно развитие (USAID), Агенцията на Корпуса на мира, Консултативната комисия по публична дипломация (ACPD), Агенцията за търговия и развитие на САЩ (USTDA), Агенцията за глобални медии на САЩ (USAGM); институции за развитие: Millennium Challenge Corporation, Overseas Private Investment Corporation (OPIC), U.S. International Development Finance Corporation (DFC), Inter-American Fund (IAF).Освен това американските мозъчни тръстове и неправителствени организации играят важна роля в публичната дипломация на САЩ, определяйки глобалния дневен ред. Това става възможно благодарение на мрежата от възпитаници, организирането на научни и експертни семинари и връзките на американски структури с международни консултантски компании. Публичната дипломация на САЩ е насочена към насърчаване на ценности, като правата на човека, демократизацията и върховенството на закона. Целевата аудитория на американската публична дипломация е две групи: настоящи и бъдещи елити и лидери, както и децата на елитите; добре образовани хора, които нямат възможност за самореализация. Във всички държави по света, където се провежда публична дипломация на САЩ, се работи както с тези, които подкрепят правителството, така и с опозицията. Така винаги има редица ешелони (първи, втори, трети, четвърти), на които могат да разчитат в бъдеще проводниците на американската публична дипломация [1].

„Тук става дума за дипломатическа работа с гражданските структури и с общественото мнение на гражданското общество в страната на акредитация. Тук става дума за комуникация с не-държавни актьори в държавата на дипломатическия мандат, пренебрегвайки донякъде Виенската конвенция за дипломатическите отношения от 1961 г., където е записано, че дипломацията не взаимодейства с гражданската публика, а само с държавните публични власти“ [4: 39].

И така, теорията за меката сила е в основата и на публичната дипломация, и на психологическата война. Наскоро стана популярен и свързаният с войната в Украйна (нежно наричана СВО – специална военна операция) термин „ИПСО“ („информационнопропагандна специална операция“). Както вече беше казано, публичната дипломация е широко понятие, даващо просторно поле за всякакви творчески изяви, а границите с психологическата война, шпионажа и намесата във вътрешните работи на чужда държава са тънки, почти незабележими и са формулирани само на академично ниво.

Меката сила на държавата представлява потенциалната възможност на една държава да разгърне „творческите си способности в областта на публичната дипломация“. Тя има и показатели, с които да бъде измерена.

Така например според Brand Finance, Global Soft Power Index 2024, България заема 64-то място от 193 държави – членки на ООН. В рамките на Балканите България е на 6-о място след: Турция – 25-о място в ООН, Гърция – 36-о, Хърватия – 47-о, Словения – 56-о, и Румъния – 58-о. След нас са Сърбия – 75-о, Албания – 92-ро, Черна гора – 102-ро, Северна Македония – 109-о, и Босна и Херцеговина – 111-о място [6].

Позиционирането на България в Global Soft Power Index 2024, от една страна, показва, че трябва да се работи упорито за подобряване на възможностите (през последната година сме отбелязали спад с -1,1 пункта), а от друга страна, показва, че и от тази позиция има възможности за разгръщане на публична дипломация в някои държави от непосредствен интерес, каквато е например Северна Македония.

Видими резултати от такова разгръщане засега не се наблюдават.

Литература

1. **Великая,** А. (2023). Публичная дипломатия России и США. – В: *Аналитический* меморандум. [онлайн]. [accessed 3.04.2025] *https://www.hse.ru/data/2023/11/15/2107470242/Меморандум_А_Великая_публичная_дипломатия_России_и_США_.pdf*.
2. **Макиавели,** Н. Флорентински истории. София: Милениум, 2020. ISBN 978-954-515-525-3.
3. **Пономарева,** Е., М. Младенович. Публичная дипломатия России. Балканское направление. – В: *Международная* жизнь, 2016, 4, с. 153 – 166. [онлайн]. [accessed 3.04.2025]. *https://interaffairs.ru/virtualread/ia_rus/42016/index.html#/153/zoomed*.
4. **Попов,** Здравко. (2021). Въведение в публичната дипломация. [онлайн]. [достъпен 3.04.2025]. *https://bdi.bg/data/pdf/ДИ_Публична%20дипломация_ОПДУ_2021.pdf*.
5. **Alinsky,** Saul D. (1971). Rules for radicals: a practical primer for realistic radicals. New York: Random House. ISBN 0-394-44341-1. [online]. [accessed 3.04.2025]. *https://historyofsocialwork.org/1946_Alinsky/1971%20-%20Saul%20Alinsky%20-%20Rules%20for%20Radicals%20-%20OCR.pdf*.
6. **Brand** Finance, Global Soft Power Index 2024. The ranking of all 193 member states of the United Nations, scored out of 100, according to the results of a survey of 170,000+ respondents in 100+ markets. [online]. [accessed 3.04.2025]. *https://static.brandirectory.com/reports/brand-finance-soft-power-index-2024-digital.pdf*.
7. **Council** on Foreign Relations. What Is Soft Power? (2023). [online]. [accessed 3.04.2025]. *https://education.cfr.org/learn/reading/what-soft-power*.
8. **Cull,** Nicholas J. (2022). Diplomacia Pública: Consideraciones teóricas. – In: *Revista* Mexicana De Política Exterior, No. 85, (marzo): 55-92. [online]. *https://revistadigital.sre.gob.mx/index.php/rmpe/article/view/690*.
9. **Longley,** Robert. An Introduction to Psychological Warfare. – In: *ThoughtCo,* Jun. 26, 2024. [online]. [accessed 3.04.2025]. *https://www.thoughtco.com/psychological-warfare-definition-4151867*.
10. **Taylor,** Philip. (2015). Public Diplomacy, Propaganda and Psychological Operations. What is Public diplomacy? [online]. [accessed 3.04.2025]. *https://www.slideshare.net/slideshow/what-is-public-diplomacy/49248837*.

ИНСТИТУЦИОНАЛЕН АНАЛИЗ НА СЪВРЕМЕННОТО МИТНИЧЕСКО РАЗУЗНАВАНЕ

д-р Ивайло Младенов
Висше училище по сигурност и икономика – Пловдив

INSTITUTIONAL ANALYSIS OF MODERN CUSTOMS INTELLIGENCE

Ivaylo Mladenov, PhD
Higher School of Security and Economics – Plovdiv

Резюме: *Задълбоченото научно изследване на теоретичните постановки, свързани с разузнаването като социален феномен, както и аналитичният преглед на вътрешноведомствената структура и нормативно регулираното съдържание на съвременното митническото разузнаване водят до откроването на безспорния извод, че то е специфична проява на институционално обособена разузнавателна активност.*

Ключови думи: *Европейски митнически съюз; митническо разузнаване; Агенция „Митници“; национална и съюзна сигурност*

Abstract: *The in-depth scientific study of the theoretical propositions related to intelligence as a social phenomenon, as well as the analytical review of the internal departmental structure and the normatively regulated content of modern customs intelligence lead to the undisputed conclusion, that it is a specific manifestation of institutionally distinct intelligence activity.*

Key words: *European Customs Union; customs intelligence; Customs Agency; national and union security*

Разузнаването като специфично и тайно обществено явление се характеризира със своето многостранно развитие и дълбочина на реализацията си, особено през последното столетие, като целенасочено се концентрира върху опазването на сигурността на участниците в глобалното конкурентно пространство [8: 28]. Първоначално проявено като военно, то постепенно обхваща в дейността си всички важни политически събития, икономическия потенциал, естествените ресурси и прониква в ценностната система, морала и волята на дадена нация за осъществяването на набелязаните цели и постигането на мащабни стратегии [13: 9].

След трагичните събития на 11.09.2001 г. в САЩ и другите терористични атаки в Европа опазването на сигурността се превърна в един от главните приоритети на Митническия съюз. Сигурността на ЕС, както и на държавите членки, а също и на техните граждани, е вече в пряка зависимост от прецизността в работата на всеки граничен пункт, през който стоките влизат в Съюза. Ако тези администрации не са в перманентно състояние да се справят с рисковете и заплахите по външните граници на Съюза, то както единният пазар, така и цялата Общност няма да могат правилно да функционират [22: 3].

Тези потребности наложиха на Митническия съюз необходимостта от въвеждането в експлоатация на новаторски и комплексни технологични решения, които да рационализират крайната ефективност на надзорните и контролните въздействия, с подчертано превенциален акцент. Динамичната проява на тази тенденциозност е структурирането и целенасоченото изграждане на вътрешносистемна мрежа от звена, занимаващи се с разузнавателна по характер дейност. Тези своеобразни организаци-

онни единици имат предоставени правомощия, доста различаващи се от традиционните митнически институционални форми, но също така са и изрично регулирани от правните норми. Информационно-събирателната и въздействаща активност, присъща за тях, няма самообслужващ характер, а цели решаването както на вътрешни, така и на обществено полезни задачи – нещо, присъщо и на конвенционалните разузнавателни системи [17: 61]. Затова те са законово структурирани в митническия орган като вътрешнонеобходим осведомителен компонент за почти всяко водено административно или наказателно производство.

При продължително осъщественото емпирично наблюдение върху дейното съдържание на разузнавателната функция на митническата администрация, както и при изучаването на нормативната регламентация в тази област в национален и съюзен план се синтезира следната дефиниция, разкриваща неговата институционална същност:

Съвременното митническо разузнаване е легитимно обособена, ведомствено специализирана разузнавателна инфраструктура от легален характер, която не е част от международната разузнавателна общност, но е съществен елемент от националната и съюзната сигурност и правов ред.

Детайлното разглеждане на въпросната тематика, съобразено и с теоретичните постулати на научните разработки, свързани с тази специфична и умишлено прикрита социална практика, налага следните пояснения относно даденото определение:

Легитимността на всяко разузнаване, включително и на митническото, произтича от правния му статут [2: 43] като целенасочено създадена от държавата структура въз основа на законодателна инициативност. Институционалната рамка на разузнавателната функция на митническия орган се изгражда и утвърждава както от националните, така и от европейските регулации. Отражение оказват и нормите, определящи функционалните характеристики на правоохранителните и правораздавателните юрисдикции. Поради високата степен на законодателна динамичност формата на проявление на тази специфична разузнавателната активност търпи перманентна промяна в съответствие и с негативните тенденции в развитието на транснационалните и националните криминогенни фактори.

Суверенът в лицето на изпълнителната власт има различни интереси и проявления – обстоятелство, налагащо разгъването на компетентни структури за водене на разнообразни политики, и то във всяка конкретна област. Системният анализ на тази тематика показва, че точно в стратегически важните за националния просперитет сфери на влияние се конструират и използват тясноспециализирани в предопределена насока информационно-събирателни организационни форми. Основният критерий за разграничаване между тях е кой е поръчител и/или потребител на готовия краен продукт [8: 124], като в конкретния случай това е Министерството на финансите, и поточно Агенция „Митници“.

Оттук произлиза и вътрешноведомствената същност на митническото разузнаване. То е изцяло в правомощията на митническия орган и обхваща основно задачи, свързани с перманентното и интегрирано информационно осигуряване на Агенцията. Различните разузнавателни производства, които осъществяват тези отдели, имат разнообразна степен на самостоятелност, реализацията им във времеви и пространствен аспект също не е еднаква – обстоятелство, наложено от поставените разнородни ресорни задания, както и от способите и формите на изпълнението им. Още повече че според съвременните научни разработки в разузнавателна сфера актуалните тенденции са за създаването именно на такива звена с необходимата експертност и занимаващи се с конкретна проблематика, главно от вътрешносистемно естество [18: 3].

Проучването показва, че легалният характер произтича от факта, че служителите, работещи в тази дирекция, стоят зад собствената си самоличност. Примерно при

съставянето на акт за установено митническо нарушение на базата на ЗАНН [23: чл. 37 във вр. с чл. 36] оперативните единици си написват личните имена и се подписват, като при поискване от присъстващите лица са длъжни и да се легитимират със служебната си карта [24: чл. 17, ал. 1, т. 3]. Затова е понятно, че дейността им е защитена от НК, като посегателството върху тях „при или по повод на изпълнението“ на служебните им ангажименти е квалифициращо вината обстоятелство [25] (примерно при предизвикани телесни повреди по чл. 131, ал. 2 – бел. авт.). При реализацията на високорискови задачи логично представителността им е силно ограничена, но винаги задължението за служебна легитимация остава изискуемо.

Задълбоченият анализ на тази негова индивидуалност недвусмислено показва „олекотената“ му организационна форма в сравнение с „класическите“ държавни разузнавателни служби и поради това то притежава подчертан инфраструктурен характер. Индикативен пример в тази насока е, че в дейността му няма конюнктурно политическо въздействие, има понякога и ротация на служители във или от други отдели (нещо недопустимо за специалните служби), редовият му състав няма абсолютно различаващи се индивидуални правомощия от останалия, работещ в Агенцията, а това са факти, потвърждаващи специфичната му институционална форма. Тези обстоятелства водят до отсъствието на митническото разузнаване от традиционно възприеманата национална разузнавателна общност от служби [15: 216]. Още повече че във всички държави от ЕС митническото разузнаване съществува в различни форми като организационна единица, но винаги е изградено извън полицейските и специалните служби.

Затова може да се обобщи, че липсата на митническото разузнаване в национален план води и до неприсъствието му и в международен. Тези безспорни факти обаче не са пречка за обмен на информация с вътрешните и интернационалните партньорски организации, оперираци с разузнавателна информация. Показателно е също така и участието на някои от служителите му в често структурираните междуведомствени координационни центрове за борба с различни противоправни явления с изострена степен на обществена опасност, като незаконен трафик на оръжие, наркотици, хора или акцизни стоки в сътрудничество с ГДБОП и ДАНС.

Изучаването на въпросната тематика показва, че митническата администрация от дълго време, освен събирането на приходи, изпълнява и други важни задачи от името на правителството си и допринася за постигането на национално значими цели, като закрила на обществото, улесняване на търговията, както и целенасочена защита на националната сигурност [21: 1]. Въпреки че незаконната търговия не е малка част от световния търговски обмен – между 7 и 10 % [16: 2], фискалната функция на тази администрация през новото столетие се допълва тенденциозно и от чисто правоохранителни задачи, като обществената сигурност излиза все повече на преден план. Понятието „сигурност“ институционално сега вече се тълкува в най-широк смисъл. То обхваща не само преките заплахи, свързани с престъпен, терористичен или друг вид трафик или незаконна търговия с огнестрелно оръжие, биологични продукти или експлозиви, но също така и опасностите за Общността, произтичащи от стоки, които представляват риск за общественото здраве, околната среда и потребителите [1: 54]. Отговорността за решаването точно на тези кардинални въпроси е в стратегическите приоритети на митническата администрация [26: 3], която чрез оперативните си звена по места, занимаващи се с по същество с разузнавателна по характер дейност, води до отреждането им като значим фактор за националната и съюзната сигурност.

Детайлизираното разглеждане на митническото разузнаване показва, че освен с разкриването на спецификите в институционалната му форма, неговата същност обстойно се разгадава и чрез особеностите на процесуалната му активност. В националната регламентация в сферата има уникален момент. В ЗМ изрично е подчертано, че

„Митническото разузнаване е събиране, обработка, проверка, анализ и разпространяване на информация от митническите органи...“ [24: 31].

Така, законодателно, се разкрива процесуалното съдържание на митническото разузнаване като алгоритмична поредица синхронизирани и взаимнообусловени действия. Тези активности организационно се осъществяват и приключват в съответствие с обективните измерения в динамиката на обследваните обекти. В сърцевината им стои необходимостта от перманентно придобиване, интегриране и аналитично интерпретиране на цялата актуална и потенциално интересна фактология, необходима за функционирането и планирането [9: 122] на разните разузнавателни производства. Практическото им реализиране е неосъществимо без директните и индиректните връзки, които съществуват както помежду им, така и в системен план.

Изучаването на този алгоритъм показва, че съставният и изходен пункт е събирането на информация. Коректният термин според теоретичните „догми“ в областта на разузнаването е „събиране на данни“, защото чак след придобиването и преработването им с определена цел се получава конкретно необходимата информация. Данните притежават неструктуриран характер и са пряко отражение на факти от обективната действителност [4: 186]. Събират се непосредствено – чрез допир до веществения им носител, или косвено – чрез определен инструментариум. Те могат да произлизат или от информатори, като доносници, внедрени лица или колеги, т.е. само хора могат да са информатори, или да произтичат от източници на данни [12: 5]. Такива са: предмети, отделни средства или технически системи, използвани за регистриране и предаване на сведения относно обстановката или действията на подконтролния обект или обекти. Съобразно правната регламентация за достъп до източниците те се делят на секретни, служебни и открити.

От откритите източници се получава най-съществената част от тях, достигаща до 80 % [5: 28] от общия обем. В тази плоскост първоизточници на сведения, предизвикващи разузнавателен интерес в съответствие с поставените задачи, са средствата за масова информация, печатните тиражи, електронните медии, специализираните издания, библиотечните фондове и интернет мрежата. Характерно за явните източници е, че те са за всеобща употреба и изискват най-малко средства, време и усилия за боравене с тях. Основният им недостатък е предварително неясната степен на истинност на съдържанието им и затова те никога по същество не могат да заменят останалите два вида.

За митническото разузнаване най-голямо значение имат служебните източници.

Те се разделят на вътрешни по произход за митническата администрация, като ИТ системите БИМИС, СОРИ, БАЦИС и други от този род. Разучаването на тези източници показва, че в ЗМ [24: Допълнителни разпоредби, § 1, т. 24] има интересен момент, ясно разкриващ правния статут на служебния им по характер формат, а именно, че те „не са държавна тайна, но са свързани с изпълнението на функциите и задачите на митническите органи по прилагането на митническото, валутното и акцизното законодателство“ и нерегламентираният достъп до тях „би се отразил неблагоприятно на интересите на АМ или на друг правен интерес“. Логично тези вътрешни източници притежават сравнително висока степен на достоверност на съдържанието си, но и също така подлежат на оценка.

В служебните източници от външно естество попадат случаите, когато посоката на данните има външен за системата произход, независимо дали е официален, или не, държавен или частен. В случая е важна позицията на самия обект, породил сигнала. Тук попадат обстоятелствата, когато самите икономически оператори и други лица са пряко заинтересовани или задължени да подават данни, изискуеми за конкретните разузнавателни производства. В случая е важна позицията на самия обект, породил сигнала. Тук попадат обстоятелствата, когато самите икономически оператори и други

лица са пряко заинтересовани или задължени да подават данни, изискуеми за конкретните разузнавателни производства. С оглед на промените в съюзното митническо законодателство примерно одобрените икономически оператори дори са заинтересовани да подават сигнали при установени от тях нерегламентирани отклонения от правните норми в подопечните им обекти [27]. В материален вид тези сигнали са под формата на различни справки, отчети, декларации, инвентаризационни описи и др. Събраните данни по този начин също имат служебен характер, защото съдържат факти, често разкриващи фирмена или вътрешна за определени органи дискретност.

С абсолютно тайни източници на сведения митническото разузнаване почти не работи, с изключение на моментите, когато висшият му ръководен състав борави с такива данни, и то в доста редки случаи. Това не е значим недостатък в дейността на тази вътрешноведомствена структура, защото използваната от нея технология за събиране на данни има основно преимущество пред технологията на класическото разузнаване. Така е, защото се избягва от противоречието между нерегламентираното понякога събиране на оперативни факти чрез тайни или специални методи и средства и конституционните принципи на всяка съвременна демократична държава [10: 161].

Изучаването на въпросната тематика показва, че правилно проведен, етапът на събиране на фактологичен материал води до изискуемата обезпеченост с данни на целия последващ алгоритмичен цикъл. По този начин се осигурява необходимият потенциал за информационно превъзходство на митническото разузнаване над обследваните обекти и обществени процеси, базирано именно върху оптимално събрания информационен ресурс [3: 2].

Следващият етап е обработването на събраната фактология. Това се осъществява на базата на систематизация и чрез предварително зададени и ясно определени критерии. По същество така се модулира развитието на целия последващ комплекс от действия, основано на формулирани в началния етап насоки за работа. В процеса на преработването участват както оперативните работници, така и ръководителите им, а също и аналитични звена. Разликата е в степента на обобщеност и разнообразието в обхвата на фактологичния материал [7: 51]. Нормално е критериите за подбор да се променят понякога в рамките на развоя на дейностите, отговаряйки по този начин на променящата се динамичност в обследваното събитие. Това автоматично рефлектира върху оценъчните принципи и така признаците, по които се осъществява ревизирането на фактите, се модифицират „в движение“. На този етап влиза и преводът на данните, ако, разбира се, са на чужд език. От друга страна своеобразната „филтрация“ на ненужните сведения тук е перманентен процес, но е от изключителна важност, за да не се „потопи“ практическата насоченост в излишна и безсмислена съобразно поставената цел информационна среда.

Анализът на този разузнавателен алгоритъм показва, че етапът на проверка е от изключителна важност за резултативния завършек на целия информационно-събирателен процес. На този стадий се проверява дали събраният материал е актуален с поставената задача, като се има предвид, че той може да се отнася към миналото на обследваните явления и да има значение, а също да е свързан с бъдещето, т.е. да има и прогностичен характер и също да е ценен. Преглеждат се и неговата конкретика и пълнота съобразно информационната му „плътност“. Но най-важната проверовъчна дейност е свързана с установяването на обективността и достоверността му. Това произтича от факта, че използването поради грешка или пропуск на неистински или неверни данни може да има тежки, дори необратими последствия, произтичащи от взимането на неправилни крайни управленски решения. Тази опасност най-често е свързана с попадането на дезинформация в потока от сведения[26]. Понякога, макар и рядко, това има случаен характер, но в преобладаващите случаи се цели умишлено поставяне

в заблуждение и формиране на неверен разузнавателен облик на обекта. Понеже това е предварително модулиран процес и е в полза на нарушителя, навременното отстраняване на въпросния „информационен шум“ е от стратегическа важност.

Последният проверовъчен елемент на този стадий е на количествените параметри на събраните дотук сведения съобразно поставената задача. Ревизира се достатъчността на данните и се прави логическо обосновано заключение дали те са над практическия минимум, с който да се разбере иманентната същност на качествените характеристики на разузнавания обект. При недостатъчност информационно-събирателният процес целеустремено отново се рестартира от начален стадий.

Детайлното изучаване на въпросния разузнавателен алгоритъм, осъществяван от митническите екипи, функциониращи в тази област, показва, че с приключването на етапа на проверката се финализира стадият на първична обработка на събраните материали, като те са филтрирани, систематизирани, с отстранени непълноти и противоречия и имат висока степен на достоверност и точност. В резултат на тези целенасочени и последователно осъществени действия събраните и обработени сведения са придобили вече качеството на първична разузнавателна информация и са подготвени за най-сериозния момент от целия алгоритмичен цикъл, какъвто е анализът. В методологичното реализиране на тази дейност има подчертано научен характер и се изразява в мисловното разчленяване на изследвания обект, събитие или процес на съставните му елементи съобразно спецификата в изискванията на поставените предварително цели. Основните различия между разузнавателния анализ – изпълняван от митническите органи, и научния анализ се свеждат до по-голямата ограниченост във времевата рамка за извършването му, подчертаната краткост в обосновката на съдържателната му част, осезаемата му на моменти неопределеност (колкото и ясен да е ограничителният стремеж в този аспект), концентрацията му в точно зададена проблематика и ясната разузнавателна насоченост [20: 3]. На практика аналитичната работа се осъществява или индивидуално от определена оперативна единица, или групово чрез сформиран предварително за целта екип.

Изследването на въпросния разузнавателен цикъл показва, че след приключване на анализа, независимо в каква форма и вид е осъществен той, производната величина на първичния информационен масив е фактологически пречистена, пълноценна и потребна за последваща кумулация на информационната база [13: 212]. Така полученият в края на този изследователски по своя характер процес завършен информационен продукт е готов за разпространение. Крайният аналитичен материал се предава под формата на различни справки, бюлетини, доклади. Едни от тях се изпращат в определени звена в разузнаването, други имат силата на ведомствени документи, а трети са доказателствен материал. Всичко зависи от това кой е поръчал информационно-събирателния цикъл и съответно какви всъщност са резултатите от него. При установени отклонения от изискуемата правна форма се уведомяват разследващите органи в митническата система или прокуратурата и започва досъдебно производство. При необходимост се сигнализират органите на МВР за съвместно координирани действия със задача доизясняване на конкретния проблемен случай. По линия на международното сътрудничество често така събраната и обработена информация се обменя чрез МИС за координация на съюзно ниво, когато преследваните цели са от такъв характер. Намерение тук е готовият продукт да достигне в изискуемата форма и в най-кратки срокове до крайните консуматори. Този финализиращ етап придава известна теоретична стойност на целокупно извършения до този момент цикъл на работа, защото подпомага поне на теория вземането на правилните управленски решения [14: 23].

Проучването на разузнавателната активност на митническия орган е безспорно, че тя не приключва на практика след завършването на който и да е информационен цикъл, а продължава със старателното архивиране на събраните материали. Макар и неуреден законово, този процес се осъществява във всяка служба независимо от предмета ѝ на дейност и е форматиран по същество от подзаконови актове, като вътрешни инструкции и заповеди. Извършва се на хартиен или електронен носител по предварително определен начин и място. Събраната информация се архивира примерно по направления, по които е зададена, като акцизна, валутна, митническа или по обектов признак. Този подход спомага и за последващ контрол или оценка на цялостната ефикасност на самата работна продуктивност. Така архивираните данни често се използват впоследствие при последваща форма на разузнавателно настъпление, когато обследваните процеси имат продължителен времеви цикъл или повторяема девиантност. За по-голяма рационалност такава архивирана информационна база притежават както централните, така и местните структури, като при необходимост тя се обменя или допълва циклично. Този полезен базов ресурс от данни се явява държавна собственост и в частност на АМ, като до това важно място имат достъп само определени единици, и то с различни нива на допуск. По този начин се избягва нерегламентираният достъп, както и достигането до част или до цялата информация за разработените в нея подконтролни обекти.

Разглеждането на въпроса, свързан с разузнавателния цикъл, показва, че последният му етап е обратната връзка. Получената чрез нея насрещна информация служи за теоретично реферирање на резултатните стойности на изготвения разузнавателен продукт. В смисловото си съдържание това е съвместна дейност между оперативното звено или единица, изготвила крайната разузнавателна форма, и нейните клиенти. Обсъжда се векторът на полезност от завършения вече цикличен алгоритъм. По този начин прецизността на алгоритмичните дейности периодично се адаптира в пряка корелация с трансформациите в оперативната обстановка и произтичащите от това потребности на взискателите на обработените за тази цел сведения.

В заключение при направения обстоен преглед на съставните елементи на митническото разузнаване от гледна точка на информационно-събирателния цикъл, както и при конфигурирането на съдържателната му дефиниция, може да се обобщи следното: Един от най-показателните начини за разбиране на обществено значимия характер на съвременното митническо разузнаване е именно обстоятелственото разкриване на взаимносвързаните етапи в информационно-събирателния алгоритъм, перманентно изпълняван от оперативните или ръководните митнически екипи.

Литература

1. **Арабаджиев,** Н. Администрация на сигурността и отбраната. София: Военно издателство, 2007.
2. **Асенов,** Б. Теория на разузнаването. София: Албатрос, 2005.
3. **Балабанов,** С., Р. Илиев. (2014). Информационните способности – важен елемент от интелигентната отбрана. [онлайн]. [достъпен 11.11.2015]. *http://www.atlantic-bg.org/bg/news.*
4. **Вълев,** С. Относно дефинирането на понятието „разузнавателна информация“ в променящата се среда за сигурност. – В: *Годишник* на Военна академия „Г. С. Раковски“, 2013, № 2.
5. **Геров,** Р. Използване на откритите източници на информация във военното разузнаване. – В: *Годишник* на Военна академия „Г. С. Раковски“, 2013, № 1.
6. **Драганов,** А. Противодействие на разузнавателната дейност. Варна: ВСУ „Черноризец Храбър“, 2001.
7. **Дячки,** С. Информационна и аналитична дейност на специалните служби за сигурност. София: Албатрос, 2001.
8. **Йончев,** Д. Разузнаване. София: Фидес-Ай енд Кей, 2005.

9. **Манева,** К., Й. Русева. Конкурентното разузнаване – обективна необходимост за съвременния бизнес. – В: *Научни* трудове на Русенския университет, 2010, том 49, серия 5.1.
10. **Минева,** С. Митническо и финансово разузнаване. Варна: ВСУ „Черноризец Храбър“, 2012.
11. **Радулов,** Н. Епистемологичен подход, разузнаване и разузнавателен анализ. [онлайн]. [достъпен 9.09.2014]. *http://www.sigurnostta.com/Nauchni_statii.*
12. **Ронин,** Р. Своя разведка. Минск: Харвест, 1997.
13. **Търкаланов,** Ю. Разузнавателен анализ. София: Албатрос, 2003.
14. **Хаджиев,** А. Външно разузнаване по отношение на националната сигурност. – В: *Научни* доклади по курсантската „Еразъм“ мобилност през академичната 2012/2013 г. по Програма на Европейския съюз – „Еразъм“. София: Академия на МВР.
15. **Христов,** П. и кол. Разузнавателна защита на конституционния ред в демократичната държава. Варна: ВСУ „Черноризец Храбър“, 2011.
16. **DCAF** – Geneva Centre for the Democratic Control of Armed Forces (DCAF – Backgrounder Series). Intelligence Governance. [online]. *http://www.dcaf.ch*.
17. **McDowell,** Don. Analysis and Management Style. The Missing Link Between Vision and Decision (1992). – In: *McDowell.* Strategic Intelligence & Analysis. Selected Writings by Don McDowell. The Intelligence Study Center, 2000, pp. 40-45. [online]. *www.intstudycen.com.*
18. **The** Intelligence Study Center. (2000). [online]. *http://www.intstudycen.com.*
19. **Vanasse,** B. Top Mistake of New Intelligence Analysts. (2002). [online]. *www.humansource.com.*
20. **World** Economic Forum. New Models for Addressing Supply Chain and Transport Risk. An initiative of the Risk Response. Network, 2012.

Нормативни актове

21. **Декларация** от Аруша (ревизирана) на Съвета за митническо сътрудничество относно доброто управление и интегритета в митниците. Съставена в Аруша, Танзания, на 7.07.1993 г., на 81/82 сесия на Съвета и ревизирана през юни 2003 г. на 101/102 сесия на Съвета за митническо сътрудничество.
22. **Европейска** комисия. Съобщение на Комисията до Европейския парламент, Съвета и Европейския икономически и социален комитет относно управлението на риска в областта на митниците и сигурността на веригата от доставки, TAXUD/COM 793/2012/, окончателен, 8.01.2013 г., непубликуван в ОВ.
23. **Закон** за административните нарушения и наказания. Обн. *ДВ,* бр. 92, 28.11.1969 г.; посл. изм. и доп.
24. **Закон** за митниците. Обн. *ДВ,* бр. 15, 6.02.1998 г.; посл. изм. и доп.
25. **Наказателен** кодекс. Обн. *ДВ,* бр. 26, 2.04.1968 г.; посл. изм. и доп.
26. **Предложение** на Европейската комисия и на Съвета за изменение на Регламент /ЕО/№2913/92 за създаване на Митнически кодекс на Общността, TAXUD/COM 0452/2003/, относно Ролята на митниците в интегрираното управление на външните граници, Брюксел, 24.07.2003 г., окончателен.
27. **Ръководство** за управление на риска, сигурност и специфичен контрол. Европейска комисия, TAXUD/1450/2006/, Брюксел, 29.06.2007 г.

ОРГАНИЗАЦИЯ НА ВЗАИМОДЕЙСТВИЕТО МЕЖДУ СЛУЖБА „ВОЕННА ПОЛИЦИЯ“ И ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ“ КАТО ФУНДАМЕНТ НА ВОЕННОТО КОНТРАРАЗУЗНАВАНЕ

д-р Митко Узунов
Университет по библиотекознание и информационни технологии – София

ORGANIZATION OF INTERACTION BETWEEN THE MILITARY POLICE SERVICE AND THE STATE AGENCY FOR NATIONAL SECURITY AS A FOUNDATION OF MILITARY COUNTERINTELLIGENCE

Mitko Uzunov, PhD
University of Library Science and Information Technology – Sofia

Резюме: *Настоящият доклад разглежда организацията на взаимодействието между Служба „Военна полиция“ и Държавна агенция „Национална сигурност“ като основен механизъм за ефективно осъществяване на военноконтраразузнавателните дейности. Анализират се правните и организационните основи на това взаимодействие, както и основните предизвикателства пред неговата ефективност. Докладът акцентира върху нормативната уредба, регламентираща съвместната дейност между двете структури, и върху стратегическите аспекти на тяхното взаимодействие в контекста на националната сигурност.*

Ключови думи: *военно контраразузнаване; национална сигурност; взаимодействие; правна рамка; Служба „Военна полиция“; ДАНС*

Abstract: *This report examines the organization of interaction between the Military Police Service and the State Agency for National Security as a key mechanism for the effective implementation of military counterintelligence activities. The legal and organizational fundamental of this interaction, as well as the main challenges to its effectiveness, are analyzed. The report focuses on the regulatory framework governing the joint activities of the two structures and the strategic aspects of their interaction in the context of national security.*

Key words: *military counterintelligence; national security; interaction; legal framework; Military Police Service; SANS*

Ограничение: *При разработване на доклада да се използват само явни (публични), не класифицирани източници на информация.*

Въведение

В съвременната динамична среда на сигурност изпълнението на пълноценни контраразузнавателни дейности са от основна необходимост, която налага синхронизирани усилия и координирани действия между редица специализирани институции в сектор „Сигурност“. В този контекст Служба „Военна полиция“ и Държавна агенция „Национална сигурност“ заемат ключово място, като тяхната съвместна дейност се регламентира от междуведомствени нормативни документи, отразяващи целите на националната сигурност. Координацията между тези две институции е от голямо значение за установяването на успешна и ефективна субординация, която да осигури бърз и адекватен отговор на съвременните заплахи и предизвикателства в областта на военното контраразузнаване.

Настоящото изследване има за цел да анализира подробно механизмите, посредством които се осъществява взаимодействието между Служба „Военна полиция“ и Държавна агенция „Национална сигурност“, като се акцентира върху правните, организационните и оперативните аспекти, които определят този процес. Изследването разглежда не само положителните ефекти от изградената оперативна съвместимост, но и потенциалните предизвикателства, свързани с различията, регламентираните процеси за взаимодействие, оперативната подготовка и технологичните средства, необходими за ефективна координация [6: 94].

Чрез задълбочен анализ на нормативноправната рамка, регулираща съвместната работа на двете структури, се цели да се изведат препоръки за оптимизиране на обмена на информация и оперативната съвместимост, които да послужат като фундамент за бъдещото развитие на военното контраразузнаване в национален мащаб. Междудисциплинарният подход, който обединява правни, организационни и стратегически перспективи, предоставя възможност за цялостно разбиране на процесите на взаимодействие и за идентифициране на ключовите фактори, влияещи върху успешното им приложение. Настоящото изследване се стреми да допринесе за повишаване на ефективността на националната сигурност чрез предложението на конкретни насоки за усъвършенстване на координацията между Служба „Военна полиция“ и Държавна агенция „Национална сигурност“.

Правна рамка на взаимодействието

Организацията на взаимодействието между Служба „Военна полиция“ [2] и Държавна агенция „Национална сигурност“ се базира на нормативна уредба, която предоставя ясна рамка на съвместната дейност на двете институции [3]. Инструкцията за организацията на взаимодействието между двете структури определя основните принципи и механизми, чрез които се осъществяват синхронизиран обмен на информация, провеждане на съвместни оперативни дейности и извършване на координирани разследвания, като тези процеси представляват критични елементи в изпълнението на военното контраразузнаване. В този контекст разпоредбите, залегнали в чл. 1 и чл. 2, регулират основния процес на обмен на информация, който е насочен към идентифициране, предотвратяване и превенция на престъпления, извършени от военнослужещи или цивилни служители на Министерството на отбраната срещу националната сигурност, като по този начин се регламентират и съвместните дейности в динамичната среда за сигурност [5: чл. 1, чл. 2, ал. 1 – 2].

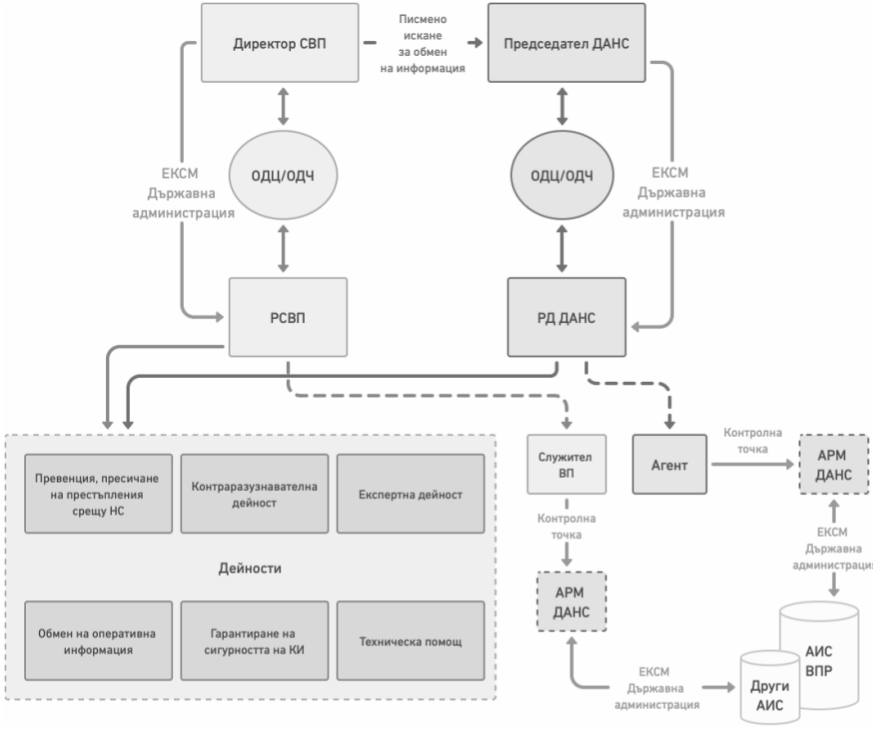
В допълнение, разпоредбите, посочени в чл. 6, уточняват специфичните задължения на всяка от страните, като предоставят насоки за изпълнение на оперативноиздирвателни и контраразузнавателни мероприятия. Тази регламентирана координация е от съществено значение за осигуряването на стратегическия характер на съвместната дейност, като позволява непрекъснат анализ и оценка на рисковете за сигурността. Защитата на класифицираната информация, която се осъществява в рамките на Министерството на отбраната, представлява друг ключов аспект на този модел на взаимодействие, като гарантира надеждността и сигурността на обменяните данни.

Нормативната уредба, регламентираща тези процеси, не само дефинира основните направления на съвместната дейност, но и предоставя методология за адаптиране към съвременните предизвикателства в областта на сигурността [5: чл. 2]. Този интегриран подход към военното контраразузнаване, базиран на стратегическа координация и синхронизирани оперативни действия, е насочен към реакция при идентифициране, превенция и неутрализиране на престъпления от военнослужещи и цивилни служители на Въоръжените сили. Регламентираният характер на взаимодействието

между Служба „Военна полиция“ и ДАНС, оформен от разпоредбите на Инструкцията, подчертава значението на установяването на стабилна и надеждна система за обмен на информация, която да допринесе за по-ефективната защита на националната сигурност в условия на непрекъснати и бързопроменящи се предизвикателства пред националната сигурност.

Изградената нормативна рамка, съчетана с високото ниво на верификация на оперативните дейности, представя изграждането на системата на военното контраразузнаване. Този модел, утвърден от Министерството на отбраната и Държавна агенция „Национална сигурност“, осигурява гъвкавост и ефективност за справяне с динамично променящите се заплахи, като същевременно гарантира защитата на класифицираната информация и оптимизира обмена на разузнавателни данни в полза на националните интереси *(Фиг. 1)* [6: 95].

Фигура 1. ***Организационна структура на взаимодействието между СВП и ДАНС***



Източник: Узунов, *Митко. Взаимодействие между подвижни групи и обекти от Въоръжените сили на Република България с групи и обекти от системата за национална сигурност. Дисертационен труд. София: УниБИТ, 2025, с. 97.*

Съвместни дейности, извършвани между Служба „Военна полиция“ и ДАНС

- Координация на дейностите и действията на оперативно и тактическо ниво относно превенцията, пресичането на замислени, подготвяни или извършени посегателства и престъпления срещу националната сигурност, реда и сигурността в състава на Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната, Българската армия и формированията на Въоръжените сили, участващи в операции и мисии извън територията на страната [5: чл. 2, ал. 1 – 2].

- Обмен на информацията.

- Надеждност и гарантиране на сигурността на класифицираната информация.

- Оказване на експертна и техническа помощ – тези дейности се извършват съвместно между служителите на двете структури по линия на разследването, превенцията и неутрализирането на извършване на престъпления срещу Републиката и националната сигурност на военнослужещи и цивилни служители в състава на Въоръжените сили.

Процеси на военното контраразузнаване

Военното контраразузнаване представлява динамичен и комплексен процес, който обхваща различни дейности, насочени към защита на националната сигурност в структурите от Въоръжените сили и критичната инфраструктура от външни и вътрешни заплахи. В основата на този процес стоят събирането, анализът и оценката на информация с цел идентифициране на злонамерени действия, разузнавателни операции и потенциални заплахи за националната сигурност. Системният подход към военното контраразузнаване изисква интегриране на различни методи на разузнавателна дейност, включително агентурни, технически и аналитични инструменти.

Значителна част от усилията в тази област са насочени към защита на класифицираната информация и предотвратяване на нерегламентиран достъп до държавна тайна. В този контекст се прилагат строги мерки за сигурност, включващи използването на криптографски технологии, контрол върху достъпа и наблюдение на комуникационните канали. Ефективното военно контраразузнаване изисква също така своевременно идентифициране и неутрализиране на диверсионни и/или шпионски дейности, които могат да представляват заплаха за националната сигурност и отбраната на страната [1: 11].

Оперативната дейност в този аспект предполага тясно сътрудничество между различните структури на сектора за сигурност, като особено внимание се отделя на координацията между военните и гражданските институции. Това взаимодействие е ключово за ефективното провеждане на междуведомствени операции, които целят своевременното и адекватно противодействие на хибридни заплахи и разузнавателни действия от внедрени агенти. Оптимизацията на комуникационните канали и обменът на информация между структурите са критични фактори за успешното функциониране на военното контраразузнаване.

Периодичните обучения и практически симулации играят съществена роля в подготовката на персонала, ангажиран в контраразузнавателната дейност. Провеждането на съвместни тренировки, базирани на реалистични сценарии, допринася за повишаване на оперативната готовност и съвместимост между заинтересованите звена. В съвременните условия на сигурност способността за бърза адаптация към нови заплахи и използването на иновативни подходи са ключови за успешното изпълнение на контраразузнавателните задачи [1: 65].

Предизвикателства пред ефективността на взаимодействието

Анализът на модела на взаимодействие между структурите, ангажирани във военното контраразузнаване, разкрива редица слабости в нормативната регулация, които създават значителни предизвикателства за ефективността на техните дейности. Сред тях се открояват следните проблеми:

- Несъвършенствата в механизмите за оперативна координация водят до увеличено време за реакция и създават условия за неефективно изпълнение на поставените цели. В настоящия модел на взаимодействие се наблюдават забавяния, произтичащи от необходимостта от одобрение на високо ниво, което води до риск от неефективност при осъществяване на тактически действия. Времето и процесът на оповестяване представляват ключови елементи за успешната реализация на междуведомствени операции, като тяхната оптимизация би подобрила значително способността за своевременно противодействие на заплахите.

- Липсата на цялостна организация и изградена Единна електронно-съобщителна мрежа (ЕКМС) възпрепятства бързия и ефективен обмен на класифицирани данни между отделните структури. Това ограничава възможността за навременно споделяне на критична разузнавателна информация, което може да компрометира процеса на вземане на решения и изпълнението на стратегически важни задачи. Създаването на модерна, сигурна и унифицирана комуникационна система би спомогнало за повишаване на оперативната ефективност.

- За осигуряване на ефективно взаимодействие между институциите, ангажирани във военното контраразузнаване, е необходимо провеждане на регулярни съвместни обучения на личния състав. Симулирането на оперативни театри с участието на различни звена би подобрило координацията и готовността за реални междуведомствени операции. В настоящия момент липсва устойчива практика за подобен тип учения, което ограничава адаптивността на силите към съвременните предизвикателства.

Заключение и изводи

Въз основа на горепосочените фактори в анализа може да се заключи, че повишаването на ефективността на военното контраразузнаване в Република България изисква цялостен подход за реформиране на нормативната рамка, усъвършенстване на механизмите за координация и комуникация, както и провеждане на редовни обучения на личния състав. Само чрез тези мерки могат да се гарантират повишаване на способностите за своевременна реакция и ефективно противодействие на съвременните заплахи за сигурността и отбраната.

Ефективността на военното контраразузнаване се определя от степента на координация между Служба „Военна полиция“ и Държавна агенция „Национална сигурност“. Съвместната им дейност трябва да бъде основен елемент за защитата на националната сигурност, като регламентира дейностите за противодействие, превенция и разследване на престъпления, извършвани от военнослужещи и цивилни служители в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, насочени към националната сигурност. Успешното осъществяване на тази дейност зависи от интегрирането на оперативни, правни и стратегически компоненти в рамките на общата система за обмен на информация и съвместни действия.

За постигането на висока оперативна съвместимост е необходимо усъвършенстване на механизмите за взаимодействие, което включва както развитие и адаптация

на нормативната уредба, така и въвеждане на съвременни високотехнологични решения и решения с изкуствен интелект, централизирайки вземането на решения и създавайки по-бързи механизми за анализ на риска.

Подобряването на правната рамка означава не само адаптиране към динамично променящите се условия, но и създаване на нови регулаторни механизми, които да улеснят обмена на данни между институциите и да гарантират надеждността на предоставената информация. От своя страна оптимизирането на оперативните процеси се основава на непрекъсната модернизация на комуникационните системи и методите на съвместна работа, които позволяват бързо и ефективно реагиране при идентифициране на рискове и заплахи.

Сегашният модел на взаимодействие, при който Служба „Военна полиция“ и Държавна агенция „Национална сигурност“ представят решение за изграждане на координация между различните елементи, създава затруднения при взимането на аргументирани решения поради високото ниво на верификация за провеждане на съвместни дейности. В резултат на това не се постига оптимално използване на ресурсите и се занижава способността на институциите да се адаптират към сложните и многопластови заплахи, характерни за съвременната динамична среда.

В заключение, ефективната координация между ключовите институции е от решаващо значение за успешното функциониране на системата на военното контраразузнаване.

Литература

1. **Велев,** Светослав и кол. Система за разузнаване. София: Военна академия „Георги Стойков Раковски“, 2023. [онлайн]. *https://rndc.bg/wp-content/uploads/2023/06/sistema.pdf.*
2. **Закон** за военната полиция. Обн. *ДВ,* бр. 48 от 24.07.2011 г.; изм. и доп. *ДВ,* бр. 18 от 1.03.2024 г.
3. **Закон** за ДАНС. Обн. *ДВ,* бр. 109 от 20.12.2007 г.; изм. *ДВ,* бр. 70 от 20.08.2024 г.
4. **Министерски** съвет. Правилник за прилагане на Закона за Държавна агенция „Национална сигурност“, приет с Постановление на Министерския съвет 23 от 11.02.2008 г. Обн. *ДВ,* бр. 17 от 19.02.2008 г.; изм. и доп. *ДВ,* бр. 40 от 7.05.2024 г.
5. **Министерство** на отбраната, Държавна агенция „Национална сигурност“. Инструкция за организация на взаимодействието между Служба „Военна полиция“ и Държавна агенция „Национална сигурност“. [онлайн]. *https://www.mod.bg/bg/doc/proekti_documenti/20171128_Instrukcia_vzaimodejstvie_DANS_SVP.pdf.*
6. **Узунов,** Митко. Взаимодействие между подвижни групи и обекти от Въоръжените сили на Република България с групи и обекти от системата за национална сигурност. Дисертационен труд. София: УниБИТ, 2025.

COLLECTION
of reports from the Scientific-Theoretical Conference
on the subject of
BULGARIAN INTELLIGENCE AND COUNTERINTELLIGENCE – CHALLENGES, PROBLEMS, PERSPECTIVES
April 11, 2025, Plovdiv

CONTENTS

ВИСШЕ УЧИЛИЩЕ ПО СИГУРНОСТ И ИКОНОМИКА
Пловдив

СБОРНИК с доклади
от научнотеоретичната конференция на тема:
БЪЛГАРСКОТО РАЗУЗНАВАНЕ И КОНТРАРАЗУЗНАВАНЕ –
ПРЕДИЗВИКАТЕЛСТВА, ПРОБЛЕМИ, ПЕРСПЕКТИВИ
11 април 2025

Българска
Първо издание

Отговорен редактор Георги Любенов Манолов
Редактор Олга Емилова Златанова
Коректор Камелия Колева Алексиева
Предпечат Камелия Колева Алексиева
Корица Камелия Колева Алексиева
Издава Издателски комплекс ВУСИ

Издателски комплекс • Дигитален печат • Рекламно студио
Пловдив, бул. Кукленско шосе 13, e-mail: pechatnica@vusi.bg; tel.: +359 884 557 841; +359 882 392 740

Пловдив, 2025

ISBN (Print) 978-619-7774-24-5
ISBN (ePub) 978-619-7774-25-2
ISBN (pdf) 978-619-7774-26-9

ИЗДАТЕЛСКИ КОМПЛЕКС ВУСИ
Пловдив, бул. Кукленско шосе 13
e-mail: pechatnica@vusi.bg
тел.: +359 884 557 841; +359 882 392 740

PUBLISHING COMPLEX HSSE
13, Kuklensko shose Blvd., Plovdiv, Bulgaria
e-mail: pechatnica@vusi.bg
tel.: +359 884 557 841; +359 882 392 740

ISBN (Print) 978-619-7774-24-5