ЗА НОВИТЕ РЕАЛНОСТИ В УПРАВЛЕНИЕТО И КОМПЕТЕНЦИЯТА „ИНФОРМАЦИОННА СИГУРНОСТ“

Димитрина Стефанова, Валентин Василев, Игор Бритченко

FOR THE NEW REALITIES IN MANAGEMENT AND “INFORMATION SECURITY” COMPETENCE

Dimitrina Stefanova, Valentin Vasilev, Igor Britchenko

Резюме: *Интензитета на промените в последните години е наистина удивителен. В такъв контекст, изискванията пред компетенциите и уменията на служители и ръководители също се интензифицира в посока на промени. От друга страна и в тази връзка, с оглед на кризите, днес управлението на информационната сигурност е необходимост за всяка организация в светлината на търсенето конкурентното предимство. На практика информационната сигурност се свързва с киберсигурността, бързоразвиваща се теория и практика, както в технологичен, така и в законодателен и програмен аспект. От гледна точка на човешкия фактор тя кореспондира с разпространение на знание, усвояване на умения и компетентности, обобщени като дигитални умения. Разработването и управлението на програми за информационна сигурност силно зависят от професионалната компетентност и експертност на човешкия ресурс и правят тази компетентност ключова за развитието на всяка организация.*

Ключови думи: *промени, кризи, управление на човешките ресурси, сигурност, компетенции.*

Summary: *The intensity of changes in recent years is truly astonishing. In such a context, the requirements for the competencies and skills of employees and managers are also intensifying in the direction of changes. On the other hand and in this connection, given the crises, today the management of information security is a necessity for any organization that considers organizational information as a valuable asset and considers it in the light of its competitive advantage. Information security is frequently associated with cyber security, a concept and field that is fast evolving on all fronts—technological, regulatory, and programmatic. From the perspective of the human factor, it corresponds to the knowledge transfer and learning abilities that are collectively referred to as "digital skills." Human resource professional competence and expertise are crucial to the management and development of information security initiatives, making them essential to the growth of any organization.*

Keywords: *changes, crises, human resource management, security, competencies.*

ВЪВЕДЕНИЕ

Промените на всички организационни нива са факт. Факт са и кризите, които предполагат и предизвикват голяма част от тези промени. От друга страна, с нарастването на обема от данни, с обхвата и усъвършенстването на информационните технологии, за съхраняването на информацията се изисква все по устойчиво концептуално мислене в посока на информационната сигурност. Това е свързано с промяната на информацията в качествено и по обем отношение и превръщането ѝ в изключително важен и ценен ресурс или обект за бизнеса и обществото.

В друг ракурс, е необходимо спазване на нормативните и законодателни изисквания за защита на данните на личността, организацията и административните нормативи.

Постигането на желаното състояние, разбирането, контролът, одитирането на информационните процеси и системи не са подчинени на обща свърхширока компетентностна основа, която включва придобиване на знания за софтуер, хардуер, човек и организационни концепции. В такъв контекст се насочва вниманието към осигуряване на подходящи мерки за защита на информация, компютърния хардуер и софтуер на организацията и сигурността. Така ще се осигури подпомагане на мисията и целите на организацията чрез превенция за предпазване на нейните физически, финансови и човешки ресурси, репутация и запазване на доверие сред клиенти и контрагенти и др., спазване на нормативни изисквания и др.

1. СЪДЪРЖАТЕЛНИ АСПЕКТИ НА КОМПЕТЕНЦИЯТА „ИНФОРМАЦИОННА СИГУРНОСТ“

Различните изследователи извеждат сходни определения за понятието информационна сигурност, като разширяват или стесняват техния диапазон и обхват, в зависимост от разясняването на свързаните основни елементи. Информационната сигурност обикновено е разбирана като техническа и е в компетентността на тесни специалисти (CNSS, 2022).

Също така, тя се разглежда като защита на информацията и съпътстващата инфраструктура от случайни или умишлени влияния от естествен или изкуствен характер. „Под информационна сигурност се разбира такова въздействие, което изключва възможността за преглед, промяна или унищожаване на информация от лица, които нямат право на това, както и изтичане на информация поради съпътстващо електромагнитно излъчване и смущения, специални устройства за прихващане (унищожаване) по време на предаване между обекти на компютърна технология. Защитата на информацията е набор от мерки, насочени към гарантиране на поверителността и целостта на

обработваната информация, както и на наличността/достъпността на информация за потребителите (Andress, 2014)“. Andress (2014) развива концепции за информационната сигурност, в чиито контекст я обособява като ежедневна грижа на организациите независимо от нейната големина. Особено внимание е необходимо да обърнат онези организации, които обработват различен вид лична информация, финансови данни, данни за здравеопазването, образователни данни или други видове данни, които се регулират от законите на страната. Според него инцидентите със сигурността на информацията са вплетени в условията за тяхното въздействие, като например нарушения на поверителността или автентичността на дадено имейл съобщение. Накратко, информационната сигурност е ключов компонент на съвременния свят (Stoykov & Vasilev, 2021).

Така например, Семерджиев и Митев (2014) предлагат рамка, която предполага, че поддържането на информационната сигурност е такова състояние на организацията, в което се осигурява, поддържа и гарантира: непрекъснатост на работните процеси; минимизация на рисковете за организацията; максимизиране на възвръщаемостта на инвестициите; увеличаване на възможностите за успех на инициативите (начинанията) и успехът зависи силно от целия човешки ресурс на организацията.

От гореизложеното следва, че информационна сигурност е свързана със защита на поверителността, целостта и наличността на информационни активи, независимо дали са в процес на създаване, съхранение, обработка или предаване. Постига се чрез прилагане на политика, образование, обучение, комуникация, одит, технологии и е жизненоважен компонент за ерата, в която данните се отнасят до безброй лица и организации и които се съхраняват в различни компютърни системи, често не под пряк контрол. Същевременно се отнася за организация, в която производството, съхраняването, преработката, продажбата и използването на информацията са основен предмет на дейност и особено в нейната висша форма – знанията. Така в случай на организация, която не отделя време, за да се постави правилно на добра основа по отношение на информационната сигурност, последиците могат да бъдат сериозни.

„Служителите и техните потребности и очаквания също са много различни в последните години. Именно поради факта, че служителите на новата епоха на знанието са с много повече и нови желания за развитие и усъвършенстване. Старият и утвърден начин на мислене и вземане на решения, основаващ се на диалога и диалектическия спор, вече не е толкова ефективен, тъй като при него се изключва съзидателното и творческото мислене“ (Василев & Стоилков, 2023, с. 68).

Цифровият преход и квалифицираната работна сила са ключови за осъществяването на бизнеса. Това насочва вниманието към подобряване на квалификацията и преквалификацията на работната ръка за работа с цифрови данни, така че да съответства на изискванията на бизнеса в съвременните условия, като основно това е в „ръцете“ на самите организации. В резултат на това се вижда, че на хората все още им е необходимо усвояване на умения за търсене, анализиране, синтезиране, оценяване, съхраняване и опазване на информацията в дигитална среда. Изследователят Ala-Mutka (2011) обобщава, че „компетентен” означава притежаване на достатъчно умения и възможност за осъществяване на ефективна дейност, която в дигитална среда се свързва с умения за работа с цифрови технологии.

Обективното оценяване на нивото на дигитална компетентност помага на мениджмънта да разбере къде и какви са пропуските, които трябва да запълнят, за да реализират личните или професионалните си цели, да се определят нуждите и насоките от обучение. Чрез повторяемост през определено време, процесът на оценяване подпомага, както цялостната оценка на ефективността на проведените обучения, вътрешните комуникации и взаимоотношения, така и ефектите върху организация. Тези компетенции са свързани с логично и точно мислене, обработване на голям обем от информация и развиване на добри комуникационни умения. Новите вариации за акумулиране и предоставяне на информация променят начина на живот, на мислене и работа в организациите. Изискванията и претенциите се мултиплицират на всички нива в обществото (Stefanova, Vasilev, & Efremovski, 2023).

Стигаме до извода, че човекът, неговата дигитална и информационна компетентност, свързана с информираността и разбирането на сигурността в това отношение, знанието за предизвикателствата на дигитализацията са с ключова роля в информационната сигурност.

Наличието на квалифицирани кадри за работа с информация и данни е другият все по-съществен аспект на информационната сигурност. Да не пропускаме, че в днешното дигитално общество се налага по-висока квалификация на мениджърите в организацията, които същевременно предявяват по-строги изисквания и към равнището и степента на образование на своите служители.

По-горе се засегнахме направленията, свързани със знанията на хората в организацията, произтичащи от информационната сигурност, които е необходимо да преминат в обща компетентност „информационна сигурност“ на служителите в организацията**.** Какво се визира в тази връзка? Понятието „компетентност“ произлиза от латински език (лат. competens -entis – „способен” (Филипова-Байрова и

др., 1993) и се използва широко в различни модели за управление на човешките ресурси.

Общата компетентност „информационна сигурност“ ще се определя като динамична съвкупност от знания, умения, нагласи и отношения за информацията, информационните процеси, системи и рисковете спрямо тях, които се придобиват и са присъщи на човешкия ресурс, ангажиран ежедневно с работния процес.

За разлика от нея специализираната компетентност ще е свързана с човешкия ресурс, пряко отговорен за поддържането на информационната сигурност. По отношение на управленската такава, тя ще включва знания и умения за **чувствителността на информацията, оценката и използването на управленски механизми за осигуряване на информационната сигурност, политика, програмен план, мониторинг, управлението на информационния риск**. В подобен контекст управлението трябва да демонстрира подходящи поведения, необходими за постигането на резултати в осигуряването на информационната сигурност или при определена професионална роля. Компетентността най-често се свързва със способност, като умение, основано на знание, свързано със защитата на информацията и всички произтичащи от нея особености спрямо ролята и значението й за организацията.

Тук ще поставим по-специален акцент върху управленската компетентност. Тя е провокирана от два основни аспекта.

На първо място в повечето дефиниции информационната сигурност се коментира пряко като част от риск мениджмънта на организацията. Това кореспондира и с най-популярния стандарт за качество ISO/IEC 27001 за **системи за управление на информационната сигурност (ISMS)**. Той насочва към изисквания по въвеждане на системата за управление на рисковете, свързани със сигурността на данните, притежавани или обработвани от организацията. Предимствата на стандарта са свързани с:

- Намаляване на уязвимостта си към нарастващата заплаха от кибератаки;
- Отговор на променящите се рискове за сигурността;
- Увереност в това, че активи като финансови отчети, интелектуална собственост, данни на служители и информация, поверена от трети страни, остават неповредени, поверителни и достъпни при необходимост;
- Осигуряване на централно управлявана рамка, която защитава цялата информация на едно място;
- Подготовка на хора, процеси и технологии в организацията да се изправят пред базирани на технологии рискове и други заплахи;

• Защита на информацията във всички форми, включително базирани на хартиен носител, базирани в облак и цифрови данни;

• Спестяване на средства, като се увеличи ефективността;

Същевременно с това тази система спазва всички добри практики и принципи, заложени в този международен стандарт, който дава насоки за създаване, внедряване, поддържане и непрекъснато подобряване на системата за управление на информационната сигурност, като не се ограничава до вида, размера и сектора на организацията. Само управленската визия може да оцени предимствата на внедряването на един или друг стандарт по качество, свързан със сигурността на информацията, а те са множество такива, както по-долу изборните такива.

Български стандарти за системи за управление на сигурността на информацията:

1/ БДС ISO/IEC 27000:2010 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник.

2/ БДС ISO/IEC 27001:2006 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания.

3/ БДС ISO/IEC 27002:2008 Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията.

4/ БДС ISO/IEC 27003:2011 Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията.

5/ БДС ISO/IEC 27004:2012 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване.

6/ БДС ISO/IEC 27005:2009 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията.

7/ БДС ISO/IEC 27006:2009 Информационни технологии. Методи за сигурност.

Познаването на стандартите и сигурността на информацията са ценен актив (Български институт за стандартизация, 2013). Информацията възприета като ценна, предопределя необходимостта от управление на огромно количество данни и тяхната защита е очевидна.

Информацията и свързаните с нея процеси, системи и мрежи представляват критични бизнес активи. Организациите и техните информационни системи и мрежи са изправени пред многобройни заплахи за сигурността, включително измами, шпионаж, саботаж, вандализъм, пожари и наводнения. Компютърните пробиви и атаки

стават по-чести, по-смели и по-сложни. На второ място **информационната сигурност определя своите политики, правила и процедури своеобразно мисията, целите и структурата на организацията.** Сами по себе си тези **водещи детайли** от **управлението на организацията изискват висока управленска далновидност. Сигурността, заявена от гледна точка на мисията на организацията, следва да обозначи ролята** на системата, да я дефинира, да определи изискванията за сигурност, заложени в тази роля. Ролите и функциите на една система може да не са ограничени до една организация. В зависимост от вида на организацията може да има една междуорганизационна система, която да включва и други участници. Предприемането на практическите дейности за управление на информационната сигурност изискват целесъобразни решения. Архитектурата на системата за управление на сигурността на информацията зависи от потребностите и целите на организацията, изискванията за сигурност, използваните за дейността процеси, големината и структурата на самата организация. Разработването и функционирането на системата трябва да отговарят на интересите и изискванията за сигурност на информацията на всички заинтересовани страни, включително клиенти, доставчици, бизнес партньори, акционери и други свързани страни.

Ръководният орган е отговорен за определяне на нивото на приемлив риск за конкретна система и организацията като цяло, като се вземат предвид разходите за информационна сигурност. Тъй като рискът за информационната сигурност не може да бъде напълно елиминиран, целта е да се намери оптимален баланс между защитата на информацията или системата и използването на наличните ресурси. От съществено значение за информационните системи и свързаните с тях процеси е да имат способността да защитават информацията, финансовите активи, физическите активи и служителите, като същевременно се вземе предвид и наличието на ресурсното осигуряване.

Познаването на регулаторната рамка, свързана, например, със Закона за защита на личните данни, със Закона за защита на класифицираната информация, със Закона за достъп до обществена информация или с Наредбата за общите изисквания за мрежова и информационна сигурност, също влизат в рамките на **системите за управление на информационната сигурност в организацията.**

Информационната сигурност се постига чрез провеждането на единна политика в областта на сигурността, система от мерки за контрол, адекватни на заплахите на жизнените интереси на организацията или личността. Терминът „сигурност на информацията“ се отнася главно за информация, определена като актив, който има

стойност, и изисква съответстваща защита – например от загуба на наличност или по отношение на конфиденциалност и интегритет (цялостност).

Системата за управление на сигурността на информацията (СУСИ) предоставя модел за създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на защитата на информационните активи.

В организационен план, критичните фактори за гарантирането на информационната сигурност са свързани основно с балансираното участие, управление, обучение, комуникация и укрепване на човешкия ресурс чрез създаване на организационната култура и на ангажимент за гарантирането на информационната сигурност на всички нива на управление (Nieles, Dempsey, & Pillitteri, 2017).

Видно е, че рисковете и заплахите, свързани с информационните активи на организацията никак не са малко по обхват, разпространение и сериозност на щетите. В литературата по кризисен мениджмънт и PR към портфолиото на кризите в отделни категории са обособени кибертероризмът, информационните и репутационни кризи. Т.нар. „нови форми“ (Василев и др., 2019, с. 114-115) на кризата, като кибертероризмът, се свързва с кражба на самоличност чрез интернет пространството – потребителски имена, пароли, банкови сметки, адреси, електронни пощи, нарушаване на авторски и сродни права, производства, държане и разпространение на порнографски материали с непълнолетни лица, проповядване или подбуждане към дискриминация, насилие, омраза, основани на раса, народност или етническа принадлежност и т.н., инфраструктурни сривове, дезинформация и фалшиви новини и т.н., които също са в организационния дневен ред (Gigauri & Vasilev, 2023, p.24).

При тези кризисни явления организациите самостоятелно не биха се справили с преодоляването им. Подобни кризи не се ограничават до конкретна област на вътрешната или външна среда на организацията, тя се прехвърля от една област в друга, разкривайки проблеми, чието рекомбиниране може да доведе до свръхопасности, не са рамкирани в определен времеви диапазон, и изглеждат като вградена уязвимост, която се проявява, избледнява, мутира и отново нанася удар върху системата. Измеренията на тези кризи са много по-големи и като загуба на финансов ресурс, брой засегнати, последствия и атакуват тотално легитимността на институциите, подкопавайки капацитета им и доверието за ефективно управление (Василев и др., 2019, с. 23-24).

Настоящото изложение поставено от гледна точка на знанията, уменията и компетентностите на висшия мениджмънт и служителите в организацията за информационна сигурност, изисква познаване, освен

на ползите от добре функционираща система от информационна сигурност, и на принципите на използване.

Съответно с или без внедрени стандарти по качество за системата за управление на сигурността на информацията, принципите запазват своята актуалност и са следните:

– ясно осъзнаване на необходимостта от сигурност на информацията;

– определяне на отговорностите по отношение на сигурността на информацията;

– ангажимент на ръководството и интерес у заинтересованите страни;

– повишаване на обществената значимост;

– оценяване на риска и установяване на подходящи механизми за контрол за постигане на приемливи нива;

– сигурност, включена като основен елемент на информационните мрежи и системи;

– активна превенция и разкриване на инциденти, свързани със сигурността на информацията;

– осигуряване на всестранен подход за управление на сигурността на информацията;

– непрекъснато повторно оценяване на сигурността на информацията и реализиране на изменения, ако е уместно.

Изследването оставено в този ракурс се превръща в тема с интердисциплинарен характер и изисква релевантен инструмент за оценка на стойност, поверителност, цялост, наличност, притежание или контрол, автентичност и полезност на информацията, както и концепциите на риск, за да се определят видовете компетентности за различните служители и начините на контрол – физически, логически и административен.

2. НЯКОИ РЕЗУЛТАТИ И ИЗВОДИ

Цифровизацията, хибридните кризи и въздействия оказват огромен тласък върху развитието на организациите, като същевременно с това поставят сериозни предизвикателства. В резултат на засиления фокус върху дигитализацията, информационната сигурност се превърна в основна грижа за организациите. Това не е случайно, защото с въвеждането на новите технологии и прехвърлянето на ключови процеси на компаниите във виртуалното пространство, уязвимостта от хакерски атаки се увеличава неимоверно.

Човешкият фактор е рисковият фактор при пробив на информационната сигурност. Факт е, че най-големите хакове на системи – банкови или държавни, като Департамента на САЩ, почти винаги са подпомогнати от вътрешен човек. Дори и несъзнателно.

Освен това, в различни изследвания се констатира, че водещите заплахи за достоверността на информацията и целостта, са породени от легитимните оторизирани потребители, на които не достига компетентност по отношение на извършваните от тях действия. Техните грешки и пропуски могат да доведат до загуба, промяна или разрушаване на значима за организацията информация. Потребителите, предизвикващи нарушения чрез неумишлени грешки в ежедневната си работа, нямат конкретни мотиви или цели при тяхното извършване. Неумишлените грешки се дължат на съдържащи се в системния софтуер и в инсталираните приложни програми заплахи за сигурността, обособени в такава група.

Умишлените човешки действия съвсем не са за подценяване. В тази група попадат заплахите от съзнателни вредителски действия на служители на организацията (настоящи или бивши) или на външни за нея лица, които целенасочено искат да й нанесат щети.

Очевидно е, че дефинирането на границите на предметната област на информационната сигурност, е задача с повишена трудност.

Определението, което се формира за информационната сигурност в тесен смисъл (на ниво отдел и организация), на фона на сигурността, цели да минимизира рисковете за организационните операции, включително мисия, функции, изображения, репутация, организационни активи, физически лица, други организации от потенциално неразрешен достъп, използване, разкриване, прекъсване, промяна или унищожаване на информация и/или информационни системи.

Задача пред всяка организация е да внедри компетентността в целия човешки ресурс като улесни организационната структура с присъщите ѝ правила на работа. Тук под компетенция се разбира специфична съвкупност от знания, умения и опит, критично мислене и възприемане на информацията, позволяващи на организацията да повиши стойността си. Като допълнение, общата и управленска компетенция включват интегрирана система от ценни, редки оперативни способности, които не могат да бъдат лесно имитирани или компенсирани с нещо друго от конкурентите. В този контекст, засилената дискусия за устойчивостта през последните години е довела и до промяна в корпоративната култура в много организации, свързана най-често с корпоративната социална отговорност.

Осигуряването на информационна сигурност е свързано с три основни групи дейности, а именно технически, човекоцентрични и организационни, които са взаимообвързани.

Човешкият фактор често е подценяван и пренебрегван в съображенията за информационна сигурност, той е слабо звено и представлява заплаха за нея. В същото време човекът-субект е

производител, носител, разпространител, но и пазител на информационната сигурност.

Политиките, обучението, мотивацията, запознаването и комуникирането с технологиите създават предпоставки за предпазване от инцидентна или преднамерена повреда или загуба на информация и прерастване в сериозни кризи за организацията, включително информационни и комуникационни такива.

Развиването на компетентност в контекста на информационната сигурност е предпоставка за минимизиране на рисковете от кризи за организацията, осъзнаване на значението на информацията в „икономиката на знанието“, осигуряване на познания за защита не само на организационна, но и на лична информация, изграждане на етични принципи при боравенето с информацията и технологиите, и не на последно място, рефлексия на хората срещу зловредно социално инженерство.

Анализът на съответните елементи на информационната сигурност, проектирани в компетентност за „информационна сигурност“ отиват отвъд границите на дигиталната компетентност, но е имплицитно заложена. Човешкият фактор, като обобщено понятие за човешка дейност се разглежда като активна и съзнателна работа по проблемите на сигурността и надеждността на информационните системи, в контекста на защита на информацията.

От друга страна, стратегиите за комуникация на лидерите влияят върху организационната автентичност (т.е. нивото на истинност, прозрачност и последователност, които служителите чувстват за своята организация), организационната идентификация и защита (Стефанова и Василев, 2022, с. 102).

Идентифицирането на критичните фактори за гарантирането на развитието на „Информационната сигурност“, кооперират балансираното участие на служителите, управлението, обучението и укрепването на човешкия ресурс, ефективните вътрешни комуникации, репутацията и ценностите в една система на бизнеспроцеси и култура, разясняващи и комуникиращи с цели, свързани с устойчивото развитие на организацията.

На национално ниво информационната сигурност, изисква защита на информационната среда на обществото, което осигурява нейното формиране, използване и развитие в интерес на гражданите, организациите и държавата и тя е част от националната сигурност.

От това произтича и овладяването на общата компетентност за информационна сигурност от гражданите. Защото „... разглеждането на националната сигурност като сложна обществена система изисква възприемането на процесите и явленията, които я съставляват в единство, цялост, взаимосвързаност и противоречивост при

създаването и предоставянето на обществото на призната обществена необходимост, обществено благо и стока (Стойков, 2022, с. 64), а информационните процеси са съставна част.

ЗАКЛЮЧЕНИЕ

Глобалното разпространение на информация засилва ефекта от последствията от „информационни кризи“, като създава възможности за скок в нивото на действията на последствията, което да достига стратегически измерения.

Това превръща съвременната среда за информационна сигурност в средство за постигане на стратегически цели и определя характерна зависимост. Силата и значението на информационната сигурност, изисква разумно, рационално и практично приложение на системен подход, с централен елемент човекът, управлението на хора, организационните структури, обучението, комуникацията, репутацията и ценностите. Сигурността не е единствено и само ангажимент на управлението и оторизираните специализирани звена, то е ангажимент на всеки служител. Един хиперсвързан свят, на растящо неравенство, може да доведе до увеличаване на фрагментацията, сегрегацията и социалното недоволство, които на свой ред създават условия за заплахи на сигурността, не само в бизнесорганизацията.

Стратегическата роля в осигуряването на информационната сигурност е на човека, на софтуера, на хардуера и на организационните процеси, обвързани в една система, без да се подценява нито един от елементите.

Следва да се изгради система за защита на информацията в информационните системи или мрежи, както и способността им да гарантират конфиденциалност, цялостност и достъпност на информацията в тях. Системата трябва да гарантира и автентичност, отчетност, безотказност и надеждност на информацията и др.

Изведените предизвикателства ще бъдат ключови в следващите години и от намирането на положителни решения за тях в значителна степен ще зависи и развитието и ефективността на организациите.

ЛИТЕРАТУРА:

Български институт за стандартизация. (2013). *Стандарти и информационни технологии*. https://bds-bg.org/bg/download/file/page-section/140 // Balgarski institut za standartizatsiya. (2013). *Standarti i informatsionni tehnologii*. https://bds-bg.org/bg/download/file/page-section/140

Василев, В., Стефанова, Д., и Черкезов, В. (2019). *Мениджмънт на кризи*. София: Пропелер. // Vasilev, V., Stefanova, D., i Cherkezov, V. (2019). *Menidzhmant na krizi*. Sofiya: Propiler.

Василев, В., и Стоилков, Е. (Юни 2023). Управление на промените чрез приложение на концепцията „паралелно мислене“ – в търсене на нови решения в кризисни времена. *Сигурност и отбрана,* (1), 64-75. https://institute.nvu.bg/sites/default/files/inline-files/2023-1-05-vasilev-stoilkov.pdf // Vasilev, V. i Stoilkov, E. (Yuni 2023). Upravlenie na promenite chrez prilozhenie na koncepciyata “paralelno mislene” – v tarsene na novi reshenya v krizisni vremena. *Sigurnost i otbrana*, (1), 64-75. https://institute.nvu.bg/sites/default/files/inline-files/2023-1-05-vasilev-stoilkov.pdf

Филипова-Байрова, М., и др. (1993). *Речник на чуждите думи в българския език*. Издателство на БАН. // Filipova-Bayrova, M. i dr. (1993). *Rechnik na chuzhdite dumi v balgarskiya ezik*. Izdatelstvo na BAN.

Семерджиев, Цв., и Митев, Н. (2014). *Норми и стандарти за управление на информационни системи*. София: Софттрейд. ISBN 9789543341627 // Smerdzhiev, Tsv., i Mitev, N. (2014). Normi i standarti za upravlenie na informatsionni sistemi. Sofiya: Softtreyd. ISBN 9789543341627

Стефанова, Д., и Василев, В. (Ноември 2022). Ефективна лидерска комуникация в мениджмънта на кризи – в търсене на комплексен модел с фокус към бъдещето. *Сигурност и отбрана,* (1), 96-104. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-09-stefanova-vasilev.pdf // Stefanova, D., i Vasilev, V. (Noemvri 2022). Efektivna liderska komunikatsiya v menidzhmanta na krizi – v tarsene na kompleksen model s focus v badeshteto. *Sigurnost i otbrana*, (1), 96-104. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-09-stefanova-vasilev.pdf

Стойков, С. (Декември 2022). Дилема на (не)сигурността и добавената стойност на образованието за сигурност. *Сигурност и отбрана*, (2), 58-81. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-04-stoykov.pdf // Stoykov, S. (Dekemvri 2022). Dilema na (ne)sigurnostta i dobavenata stoynost na obrazovanieto za sigurnost. *Sigurnost i otbrana*, (2), 58-81. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-04-stoykov.pdf

Ala-Mutka, K. (2011). *Mapping Digital Competence: Toward a conceptual understanding*. Luxembourg: Publications Office of the European Union. https://www.academia.edu/42521335/Mapping_Digital_Competence_Towards_a_Conceptual_Understanding

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Second Edition). Syngress.

https://www.academia.edu/32643426/Andress_Jason_Basics_of_Information_Security_Second_Edition

CNSS. (2022, March 2). *Committee on National Security Systems (CNSS) Glossary*. CNSSI 4009, p. 106-110. https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf

Gigauri, I., & Vasilev, V.P. (2023). Paradigm Shift in Corporate Responsibility to the New Era of ESG and Social Entrepreneurship. In A. Jean Vasile, M. Vasić, & P. Vukovic (Eds.), *Sustainable Growth and Global Social Development in Competitive Economies* (pp. 22-41). IGI Global. https://doi.org/10.4018/978-1-6684-8810-2.ch002

Nieles, M., Dempsey, K. and Pillitteri, V. Y. (2017). *An Introduction to Information Security. NIST Special Publication 800-12 (Revision 1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

Stefanova, D.P., Vasilev, V.P., & Efremovski, I.P. (2023). Re-Innovative Organizational Design: Sustainable Branding and Effective Communication – Applied Models in a World With New Borders/Without Borders. In I. Gigauri, M. Palazzo, & M. Ferri (Eds.), *Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing* (pp. 112-127). IGI Global. https://doi.org/10.4018/978-1-6684-8681-8.ch006

Stoykov, S., & Vasilev, V. (2021). Prerequisites for efficiency of human resources management in crisis situations (from classic theories to a new vision). *Politics & Security, 5*(3), 15-21. https://doi.org/10.5281/zenodo.6402953