УДК 343.1

СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

SUBJECTS OF CYBER SECURITY PROVISION

Діордіца І.В.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і процесу
Національного авіаційного університету

У статті автором було сформульовано авторське розуміння суб'єкта забезпечення кібербезпеки. Акцентовано на том, що функція підвищення поінформованості громадян про безпеку в кіберпросторі має виконуватися усіма суб'єктами забезпечення кібербезпеки. Окремої уваги заслуговує той факт, що в переліку суб'єктів забезпечення кібербезпеки відсутній національний координаційний центр. Акцентується на необхідності передбачення відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури, дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави. Незрозумілим є також невключення Національного координаційного центру кібербезпеки, а також Міністерства інформаційної політики до переліку суб'єктів забезпечення кібернетичної безпеки.

Ключові слова: кібербезпека, забезпечення кібербезпеки, суб'єкти забезпечення кібербезпеки, національні інтереси, кіберпростір.

В статье автором было сформулировано авторское понимание субъекта обеспечения кибербезопасности. Акцентировано внимание на том, что функция повышения осведомленности граждан о безопасности в киберпространстве должна выполняться всеми субъектами обеспечения кибербезопасности. Отдельного внимания заслуживает тот факт, что в перечне субъектов обеспечения кибербезопасности отсутствует национальный координационный центр. Акцентируется внимание на необходимости предусмотрения ответственности субъектов обеспечения кибернетической безопасности по защите национальной информационной инфраструктуры, действенности, комплексности и постоянства мер обеспечения кибербезопасности государства. Непонятным также остается невключение Национального координационного центра кибербезопасности и Министерства информационной политики Украины в перечень субъектов обеспечения кибернетической безопасности.

Ключевые слова: кибербезопасность, обеспечение кибербезопасности, субъекты обеспечения кибербезопасности, национальные интересы, киберпространство.

It was offered to understand under the subject of providing cyber security – a natural or legal person with certain rights and responsibilities, the state as a whole, which carries out its functions in the cyberspace through the institutions of legislative, executive and judicial power, as well as non-state institutions and individual citizens. The function of raising of the citizens' awareness of security in the cyberspace must be fulfilled by all actors who are involved in the cybersecurity maintenance. It was noted that particular attention deserves the fact that the Cybersecurity National Coordination Center and the Ministry of Information Policy are not included to the list of the cybersecurity providers. It is necessary to foresee the responsibility of the subjects of the cybersecurity providers for the protection of national information infrastructure, efficiency, integrity and continuity of measures to ensure cybersecurity of the state. It was proposed to define the establishment of a balance between the protection of the national interests in the cyber sphere, the guarantee of political, economic, military and social stability in the state and the development of mutually beneficial cooperation based on the principle of equality, the realization of constitutional rights and freedoms of man and citizen on access to information as one of the main tasks of the cyber security providers. Identifying and fixing the clear list of actors, their roles, places in cyberspace and powers will make it possible to perform their functions more efficiently, to bring to responsibility and to develop new norms or to replace existing ones with the aim of eliminating of gaps. Discussion and expansion of the terminology on cyberspace will allow society to plan its actions in a modern cyberspace more qualitatively and safely. It was considered that in the formulation of the terms it is expedient to define them in a broader sense, taking into account already existing works in such branches of science as cybernetics, informatics, informatsiology, security studies, criminal law, etc.

Key words: cybersecurity, providing of cybersecurity, subjects of cybersecurity providing, national interests, cyberspace.

Постановка проблеми. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки – як найбільш оптимальні організаційно-функціональні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [1, с. 312].

В Україні також відбувається процес формування системи кібернетичної безпеки. І, як і будь-яка система, система забезпечення кібербезпеки має в своїй структурі певні суб'єкти. Вірус Petya, яким було вражено значну кількість інформаційних ресурсів центральних органів державної влади, став індикатором відсутності в Україні національної системи кібербезпеки, виявив суттєві недоліки в організації діяльності даних суб'єктів. Відсутність ґрунтовного дослідження та абсолютна новизна і визначають актуальність теми статті.

Стан опрацювання. Зважаючи на відсутність комплексного дослідження суб'єктів забезпечення кібербезпеки та кібербезпекових питань загалом, під час написання статті в нагоді стали праці науковців у різних сферах, а саме: наукової школи В.А. Ліпкана [4–9], І.В. Тімкіна, Н.Є. Новікова [10], С.В. Мельника, В.І. Кащука [11], В.П. Шеломенцева [1–3], В.Л. Бурячок, С.О. Гнатюка, О.Г. Корченко [12–13] та інших.

Метою статті є дослідження суб'єктів забезпечення кібербезпеки, для досягнення якої були поставлені такі завдання: запропонувати авторське розуміння цього поняття, визначити суб'єктів забезпечення кібербезпекової політики та наявні проблеми налагодження ефективної взаємодії між ними.

Виклад основного матеріалу. У загальному розумінні *суб'єкти* – активні учасники відносин, які наділені певними правами, обов'язками та повноваженнями.

Беручи до уваги той факт, що кібербезпека має безпосереднє відношення до інформаційної сфери, використовуючи дефініцію, яка запропонована В.А. Ліпканом у першому Словнику стратегічних комунікацій, а саме *суб'єкт інформаційної діяльності* – юридична або фізична особа, задіяна в інформаційному процесі [7, с. 365], а також термінологію безпекової сфери, «*суб'єкти забезпечення національної безпеки* – носії конституційних прав і обов'язків – це держава, громадяни України, громадські організації та об'єднання; держава, яка здійснює функції в цій галузі через інститути законодавчої, виконавчої і судової влади, а також недержавні структури й окремі громадяни» [4, с. 338], сформулюю авторське розуміння *«суб'єкта забезпечення кібербезпеки»* – фізична або юридична особа, що наділена певними правами та обов'язками, держава загалом, яка здійснює свої функції в кіберпросторі через інститути законодавчої, виконавчої і судової влади, а також недержавні структури й окремі громадяни.

Також під *суб'єктами забезпечення кібернетичної безпеки* у проекті Стратегії забезпечення кібернетичної безпеки України було визначено державні органи (передусім, інституції сектору безпеки і оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності, які здійснюють проектування, впровадження та експлуатацію складових елементів критичних об'єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист [14]. Однак для мене стало незрозумілим невключення до зазначеного переліку фізичних осіб.

А в проекті закону України «Про основні засади забезпечення кібербезпеки України» пропонується така дефініція: *суб'єкти забезпечення кібербезпеки* – державні органи, органи місцевого самоврядування, органи управління Збройних сил України та інших військових формувань, утворених відповідно до законів України, правоохоронні органи, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки національного сегмента кіберпростору, зокрема забезпеченням кіберзахисту в рамках надання інформаційних та/або телекомунікаційних послуг. І окремо виділено поняття *«суб'єкти забезпечення кібербезпеки постійної готовності»* – це державні органи або їх підрозділи, що входять до складу національної системи кібербезпеки, сили та засоби яких спеціально виділені для перебування у постійній готовності до реагування на кіберзагрози та оперативного виконання завдань забезпечення кібербезпеки [15].

Щодо теми статті, можна зазначити, що, відповідно до чинного законодавства, основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, як це закріплено у Стратегії кібербезпеки України [16]. На перший погляд, цей перелік є досить вичерпним, але, приймаючи до уваги велику кількість державних органів, які функціонують в Україні, і тим чи іншим чином стосуються кіберпростору, зауважу, що він потребує уточнення та доповнення.

Перш за все, із застосуванням функціонального підходу зупинимося на функціях, які виконують вищезазначені органи, та на їх повноваженнях.

Відповідно до положень Стратегії кібербезпеки України:

– на *Міністерство оборони України, Генеральний штаб Збройних сил України,* відповідно до компетенції – здійснення заходів із підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

– на *Державну службу спеціального зв'язку та захисту інформації України* – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури (тобто комплексу заходів, реалізованих у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [17, с. 490]), державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

– на *Службу безпеки України* – попередження, виявлення, припинення та розкриття злочинів проти

миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

– на *Національну поліцію України* – забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;

– на *Національний банк України* – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

– на *розвідувальні органи України* – здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки. Відповідно до спеціального Закону «Про розвідувальні органи», розвідувальні органи України – спеціально уповноважені законом органи на здійснення розвідувальної діяльності [18], а саме Служба зовнішньої розвідки України, яка є державним органом, що здійснює розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах [19]; розвідувальний орган Міністерства оборони України; розвідувальний орган спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону. Також зауважу існування такого поняття, як *«кібернетична розвідка»* – добування наявних у кібернетичному просторі даних та інформації противника, моніторинг його автоматизованих систем управління, систем управління зброєю, інформаційних мереж та систем і технологічних процесів, що в них циркулюють [20].

На мою думку, функція підвищення поінформованості громадян про безпеку в кіберпросторі має виконуватися усіма суб'єктами забезпечення кібербезпеки.

Оскільки система національної безпеки є багатокомпонентною і національна система кібербезпеки є її спеціальною підсистемою, мета функціонування якої полягає у забезпеченні функціонування та розвитку цієї системи, тому логічним є проведення паралелі між основними нормативно-правовими актами та виявлення спільних і різних суб'єктів. Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства.

У ст. 4 Закону України «Про основи національної безпеки України» [21] суб'єктами забезпечення національної безпеки визначено Президента України, Верховну Раду України, Кабінет Міністрів України, Раду національної безпеки і оборони України, міністерства та інші центральні органи виконавчої влади, Національний банк України, суди загальної юрисдикції; прокуратура України, Національне антикорупційне бюро України, місцеві державні адміністрації та органи місцевого самоврядування, Збройні сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України, органи і підрозділи цивільного захисту, громадяни України, об'єднання громадян.

Проаналізувавши ці положення, зауважу, що спільними суб'єктами є тільки Національний банк України та Служба безпеки України. Видається дивним неприйняття до уваги положень вищезазначеного закону під час розробки та підписання Стратегії кібербезпеки України.

Із метою забезпечення кібербезпеки має бути створено національну систему кібербезпеки як формат співробітництва державних органів, установ, організацій, приватного сектора економіки, наукових установ і організацій, професійних асоціацій та неурядових організацій у сфері кібербезпеки, зокрема аналітичних центрів.

Основою національної системи кібербезпеки є державні органи, які, відповідно до покладених завдань, безпосередньо виконують функції із забезпечення безпеки кіберпростору України.

До участі у здійсненні заходів, пов'язаних із виявленням, запобіганням і нейтралізацією кіберзагроз, залучаються інші суб'єкти забезпечення кібербезпеки [9].

Акцентую на необхідності перегляду Стратегії кібербезпеки та доповненні її іншими важливими суб'єктами, а також чітке окреслення їх повноважень.

Взявши за основу Закон України «Про основи національної безпеки України», пропоную визначити основні *функції суб'єктів забезпечення кібернетичної безпеки:*

– вироблення і періодичне уточнення Стратегії кібернетичної безпеки України, доктрин, концепцій, стратегій і програм у сфері кібернетичної безпеки, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз національним інтересам України;

– створення нормативно-правової бази, необхідної для ефективного функціонування системи забезпечення кібернетичної безпеки, а також удосконалення її організаційної структури;

– комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових (структурних) елементів) системи;

– підготовка сил та засобів суб'єктів системи до їх застосування згідно з призначенням;

– постійний моніторинг впливу на кібернетичну безпеку процесів, що відбуваються в політичній,

соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз кібернетичній безпеці. Оскільки поняття «кібернетична безпека» є новим та загрози їй не статичні, тому актуальним є їх постійний, а не періодичний моніторинг із метою їх виявлення та попередження;

– систематичне спостереження за станом і проявами міжнародного та інших видів кібертероризму, а саме несанкціонованих дій із терористичною метою стосовно систем або мереж критичних об'єктів національної інформаційної інфраструктури, інформації, яка в них циркулює, та програмного забезпечення, призначеного для її оброблення [14];

– прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву;

– розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень із метою захисту національних інтересів України;

– запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;

– локалізація, деескалація та врегулювання конфліктів і ліквідація їх наслідків або впливу дестабілізуючих чинників;

– оцінка результативності дій щодо забезпечення кібернетичної безпеки та визначення витрат на ці цілі;

– участь у двосторонньому і багатосторонньому співробітництві в галузі безпеки, якщо це відповідає національним інтересам України;

– спільне проведення планових та оперативних заходів у рамках міжнародних організацій та договорів у сфері кібернетичної безпеки.

Окремої уваги заслуговує той момент, що в переліку суб'єктів забезпечення кібербезпеки відсутній Національний координаційний центр, який є робочим органом Ради національної безпеки і оборони України та на нього покладені безпосередні обов'язки щодо забезпечення кібернетичної безпеки України. Крім того, ще у 2002 р. при РНБО України було утворено Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки, до складу якої за посадою входять керівники чи заступники міністерств, відомств, правоохоронних органів, представники Генерального штабу Збройних сил України, державних комітетів, комітетів Верховної Ради України, наукових та дослідних установ, діяльність яких пов'язана з проблематикою інформаційної безпеки. Як вбачається, Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при РНБО України має забезпечити й вироблення пропозицій щодо визначення, коригування засад внутрішньої й зовнішньої політики у сфері забезпечення кібернетичної безпеки України [3, с. 302].

До категорії «інші суб'єкти забезпечення кібербезпеки» можу включити:

– інші державні органи;

– розпорядники інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури та інших об'єктів кібербезпеки, які провадять діяльність із надання інформаційних та/або телекомунікаційних послуг;

– незалежні організації та експерти [22].

Акцентую на необхідності передбачення відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури, дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави.

Також необгрунтованою є відсутність Міністерства інформаційної політики у переліку суб'єктів забезпечення кібернетичної безпеки, оскільки воно є головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів [23].

Наголошую на тому, що ключові завдання МІП затверджено у Програмі дій уряду, а також викладено в Коаліційній угоді, підписаній п'ятьма парламентськими фракціями Верховної Ради України. Такими завданнями є:

– розроблення стратегії інформаційної політики України та концепції інформаційної (зокрема і кібернетичної – *Д.І.*) безпеки держави;

– координація органів влади в питаннях комунікації та поширення інформації;

– протидія інформаційній агресії (кібернетичним атакам – *Д.І.*) Росії [23].

У рамках цієї статті я не буду зупинятись на штучно звужених функціях центрального органу виконавчої влади лише до окремих завдань, причому із зазначенням ще й конкретної країни. Порушення правил юридичної техніки, а також нехтування проектним підходом наперед звузили здатність цього органа суттєво впливати як на інформаційну, так і на кібернетичну політику держави.

Найбільш пріоритетним напрямом діяльності держави нині є реформування власної інформаційної безпеки шляхом створення дієвої системи кібербезпеки, розбудова якої потребує розв'язання багатьох завдань як соціального і техногенного, так і організаційного характеру.

Найактуальнішими серед цих завдань такі:

– чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподіл повноважень між ними;

– забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів;

– розробка й упровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки, а також застосування дієвих стимулів із метою залучення до такого роду діяльності фахівців високого рівня кваліфікації [13, с. 22].

Визначення та фіксація чіткого переліку суб'єктів, їх ролі, місця в кіберпросторі та повноважень уможливить ефективніше виконання їх функцій, притяг-

нення до відповідальності та можливості розроблення нових норм або зміну наявних із метою усунення прогалин. Обговорювання та розширення термінології щодо кіберпростору дасть змогу суспільству більш якісно та безпечно планувати свої дії в сучасному кіберпросторі. Під час формулювання термінів вважаю за доцільне визначати їх у більш широкому розумінні, враховуючи вже наявні напрацювання у таких галузях науки, як кібернетика, правова кібернетика, інформатика, інформаційне право, інфомаціологія, безпекознавство, кримінальне право тощо.

Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану зі:

– створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;

– впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень.

Організаційне забезпечення системи кібербезпеки характеризується місцем і роллю спеціальних суб'єктів (відповідних державних органів та їх спеціалізованих підрозділів), їх функціями, повноваженнями, а також підставами, умовами і напрямами їх взаємодії під час здійснення заходів із забезпечення безпеки у кіберпросторі [3, с. 301].

Також зауважу, що створення покращення наявних умов належного упорядкування взаємозв'язків між суб'єктами забезпечення кібернетичної безпеки, засобами та методами, що ними використовуються, а також відповідних взаємопов'язаних правових, організаційних і технічних заходів, що ними здійснюються, дає змогу підвищити ефективність системи кібернетичної безпеки [3, с. 307].

Нині одним з основних завдань діяльності суб'єктів забезпечення кібербезпеки пропоную визначити дотримання балансу між захистом національних інтересів у кібернетичній сфері, гарантуванням політичної, економічної, військової та соціальної стабільності у державі та розвиток взаємовигідного співробітництва, яке б базувалося на принципах справедливості, реалізації конституційних прав і свобод людини та громадянина на доступ до інформації тощо.

Висновки. Під суб'єктом забезпечення кібербезпеки запропоновано розуміти фізичну або юридичну особу, що наділена певними правами та обов'язками, держава загалом, яка здійснює свої функції в кіберпросторі через інститути законодавчої, виконавчої і судової влади, а також недержавні структури й окремих громадян. Функція підвищення поінформованості громадян про безпеку в кіберпросторі має виконуватися усіма суб'єктами забезпечення кібербезпеки.

Окремої уваги заслуговує той факт, що в переліку суб'єктів забезпечення кібербезпеки відсутні Національний координаційний центр та Міністерство інформаційної політики.

Необхідним є законодавче передбачення відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури [24], дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави.

Потребує розроблення Закон України «Про забезпечення безпеки об'єктів критичної інфраструктури», одним із ключових елементів якого має бути державна політика у сфері безпеки інфраструктури – безпекоінфраструктурна політика.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.

2. Шеломенцев В.П. Формування законодавчих основ забезпечення кібербезпеки України / В.П. Шеломенцев // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

3. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2. – С. 299–309.

4. Ліпкан В.А., Ліпкан О.С. Національна і міжнародна безпека у визначеннях та поняттях / В.А. Ліпкан, О.С. Ліпкан. – Вид. 2-е, доп. і перероб. – К.: Текст, 2008. – 400 с.

5. Ліпкан В.А. Національна безпека України: [навчальний посібник] / В.А. Ліпкан. [2-ге вид.]. – К. : КНТ, 2009. – 576 с.

6. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні: [моногр.] / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян / за заг. ред. В.А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2015. – 664 с.

7. Стратегічні комунікації : [словник] / Т.В. Попова, В.А. Ліпкан ; за заг. ред. доктора юридичних наук В.А. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. – 416 с.

8. Діордіца І.В. Поняття та зміст національної системи кібербезпеки / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki.

9. Ліпкан В.А., Діордіца І.В. Національна система кібербезпеки як складова системи забезпечення національної безпеки України / В.А. Ліпкан, І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/natsionalna-sistema-kiberbezpeki-yak-skladovoyi-sistemi-zabezpechennya-natsionalnoyi-bezpeki-ukrayini.

10. Тімкін І.Ф. Новікова Н.Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України / І.Ф. Тімкін [Електронний ресурс]. – Режим доступу : er.nau.edu.ua.

11. Мельник С.В., Кащук В.І. Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

12. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки / В.Л. Бурячок, С.О. Гнатюк, О.Г. Корченко // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

13. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / Ред. В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
14. Стратегія забезпечення кібернетичної безпеки України (Проект) [Електронний ресурс]. – Режим доступу : www.niss.gov.ua/public/File/2013_nauk.../kiberstrateg.pdf.
15. Проект закону України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=55657&pf35401=348091.
16. Стратегія кібербезпеки України від 15.03.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016.
17. Світова гібридна війна: український фронт : [монографія] / за заг. ред. В.П. Горбуліна. – К. : НІСД, 2017. – 496 с.
18. Про розвідувальні органи України : Закон України від 22.03.2001 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2331-14.
19. Офіційний сайт служби зовнішньої розвідки України [Електронний ресурс]. – Режим доступу : http://szru.gov.ua.
20. Куцаєв В.В., Живило Є.О., Срібний С.П., Черниш Ю.О. Розширення термінології сучасного кіберпростору / В.В. Куцаєв, Є.О. Живило, С.П. Срібний, Ю.О. Черниш [Електронний ресурс]. – Режим доступу : mino.esrae.ru/pdf/2014/3Sm/1387.doc.
21. Про основи національної безпеки : Закон України від 19.06.2003 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/964-15.
22. Худинцев С. Формування державної політики у сфері кібербезпеки, реалізація Стратегії кібербезпеки України. Актуальні аспекти захисту інформації в державних ІТС [Електронний ресурс]. – Режим доступу : forum.e.gov.ua/.../Худынцев/Kiberbezpeka_Khydunzev.ppt.
23. Офіційний сайт Міністерства інформаційної політики [Електронний ресурс]. – Режим доступу : Mip.gov.ua.
24. О безопасности критической информационной инфраструктуры Российской Федерации : Закон РФ от 26 июля 2017 г. № 187-ФЗ [Електронний ресурс]. – Режим доступу : www.kremlin.ru.