УДК 342.9

Діордіца І. В.,
кандидат юридичних наук, доцент,
голова Інституту адміністративного правосуддя
Глобальної організації союзницького лідерства

ПОНЯТТЯ ТА ЗМІСТ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

CONCEPT AND CONTENT OF SUPPORT CYBERSECURITY

Автором було здійснено аналіз поняття та змісту системи забезпечення кібербезпеки. Акцентовано увагу на відсутності уніфікованого визначення та запропоновано авторське розуміння. Визначено, що завданням системи забезпечення кібербезпеки є створення необхідних умов у кіберпросторі, за яких можливим є досягнення загальнодержавних цілей і реалізація інтересів, завдань та цілей її елементів. Окремо приділено увагу суб'єктам та об'єктам системи і зауважено, що незрозумілим є невключення Верховної Ради України до цього переліку. Резюмовано, що побудова дієвої системи забезпечення кібернетичної безпеки України вимагає коректного і точного визначення державної політики у цій сфері, випереджального правового реагування на динамічні зміни, що відбуваються у кіберпросторі.

Ключові слова: *кібербезпека, забезпечення кібербезпеки, система кібербезпеки, система забезпечення кібербезпеки, кіберпростір.*

Автором был осуществлен анализ понятия и содержания системы обеспечения кибербезопасности. Акцентировано внимание на отсутствии унифицированного определения и предложено авторское понимание. Определено, что задачей системы обеспечения кибербезопасности является создание необходимых условий в киберпространстве, при которых возможно достижение общегосударственных целей и реализация интересов, задач и целей ее элементов. Отдельно уделено внимание субъектам и объектам системы и отмечено, что непонятным является невключение Верховной Рады Украины в данный перечень. Резюмировано, что построение действенной системы обеспечения кибернетической безопасности Украины требует корректного и точного определения государственной политики в этой сфере, опережающего правового реагирования на динамические изменения, происходящие в киберпространстве.

Ключевые слова: *кибербезопасность, обеспечение кибербезопасности, система кибербезопасности, система обеспечения кибербезопасности, киберпространство.*

It was offered to understand under the system of ensuring of the cybersecurity the set of organizational united bodies of management, namely governmental bodies, public organizations, officials and individuals, which direct their activities on protection of the cyberspace against cyber-attacks, forces and methods and means which are used for the goal achievement within the legislation of Ukraine. It was noted that the creation of the necessary conditions in the cyberspace, in which is possible to achieve the all-national objectives and implementation of interests, goals and aims of its elements is the task of the system of the ensuring of the cyber security. It was argument that the omission of the Verkhovna Rada of Ukraine to the list of subjects that form the basis of the national cyber security system is unclear. It was marked that the cybersecurity is the object the system of ensuring of the cybersecurity. It was stated that the building an effective the system of ensuring of the cybersecurity requires correct and accurate determination of the public policy in this area and advancing legal response to the dynamic changes which are taking place in the cyberspace. It was marked that learning of the cyber security as a whole is an entirely new phenomenon, therefore the need and viability of thorough research of the system of ensuring of the cybersecurity is visible.

Key words: *cybersecurity, ensuring of cybersecurity, cybersecurity system, system of ensuring of the cybersecurity, cyberspace.*

Інтеграція України до світового кіберпростору призвела до утворення перманентних джерел загроз національним інтересам, пов'язаним із функціонуванням комп'ютерних мереж та систем. Це спричиняє необхідність у концептуальному переосмисленні нової кібербезпекової реальності, впорядкуванні інформаційного законодавства відповідно до сучасних тенденцій розвитку інформаційних відносин з урахуванням необхідності створення умов для реалізації національних інтересів у цій сфері, зокрема розбудови систем ефективного нормативно-правового регулювання. На цю обставину також вказує і О.О. Черноног, який пов'язує розвиток національної системи кібербезпеки з будовою внутрішнього нормативно-правового поля [1].

Зважаючи на події із втручанням у комп'ютерні мережі під час президентських виборів у США, Франції, а також Указ Президента України від 18 травня 2017 р. стосовно запровадження санкцій щодо окремих фізичних та юридичних осіб, яким провайдерів в Україні зобов'язали припинити доступ до соціальних мереж «ВКонтакте», «Одноклассники», «Яндекс», проблема кібербезпеки дедалі більше потребує уваги державної інформаційної політики.

Отже, дослідження поняття і змісту системи забезпечення кібербезпеки є не лише новим у теоретичному плані, а й актуальним.

Дослідження кібербезпеки загалом є доволі новим явищем, тому акцентуємо увагу на необхідності і перспективності проведення ґрунтовного дослідження системи забезпечення кібербезпеки. Нині існують лише поодинокі статті, які певним чином стосуються теми дослідження. Щодо науковців, які вивчали цю тему, слід зазначити наукову школу В.А. Ліпкана [2–5], котрий розвивав безпекознавство ще з 2003 р. і далі успішно цим займається з метою вирішення наукових і законодавчих проблем у сфері національної безпеки, стратегічних комунікацій, зокрема кібербезпеки. Також варто

назвати О.О. Черноногa [1], В.П. Шеломенцева [6], В.Л. Бурячок, С.О. Гнатюк, О.Г. Корченко [7] та ін.

Метою статті є дослідження поняття і змісту системи забезпечення кібербезпеки, для досягнення якої були поставлені такі завдання: запропонувати авторське розуміння цього поняття, оскільки відсутня уніфікована дефініція, проаналізувати наявні дефініції, визначити суб'єктів та об'єкт системи, окреслити актуальні проблеми.

Нині провідні держави світу і суспільство загалом дедалі більше покладаються і, відповідно, залежать від безперешкодного функціонування п'ятого простору – кіберпростору, під яким пропонується розуміти сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз і банків даних, що обробляються у комп'ютерних мережах і пов'язаній із ними інфраструктурі, разом з об'єктами, що підпадають під їхній контроль та управління. Захист інтересів держав і громадян у кіберпросторі стає життєво важливим інтересом, що перетворює безперешкодне використання ІТ-мереж на суттєве питання безпеки й оборони.

Нині слід визнати, що потенційна небезпека може загрожувати системам державного і військового управління, економіки та промисловості. Україна інтегрована у світовий кіберпростір і, відповідно, зазнає різних загроз і негативних впливів, пов'язаних із його розвитком (зокрема, від наслідків суперництва США і ЄС із РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави, вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки. Найбільш ефективним шляхом вирішення зазначених питань є побудова національної моделі кібербезпеки і розробка першочергових напрямів діяльності державного та приватного секторів у сфері кібербезпеки [1], а також ефективне функціонування системи забезпечення кібербезпеки.

Починаючи з 2010–2011 рр. органи державної влади України здійснили декілька спроб реформувати (шляхом прийняття комплексного профільного нормативно-правового документа) механізми забезпечення кібербезпеки держави. Одним із завдань цього процесу було утворення замість переважною мірою ситуативних відносин між структурами, що забезпечують кібербезпеку, чіткої та зрозумілої системи їх взаємодії. Це мало уможливити створення «національної системи кібербезпеки України» (відповідне завдання було поставлено, зокрема, в Стратегії національної безпеки України в редакції від 2013 р. [8] та продубльовано у Стратегії кібербезпеки України від 15 березня 2016 р.).

Неконтрольоване поширення і необмежене застосування інформаційного і кіберпросторів протягом останніх десятиріч:

1) призвело до уразливості інформаційної сфери більшості країн світу для стороннього кібернетичного впливу;

2) визначило політичну необхідність контролю і подальшого регулювання відносин у цій царині;

3) дало підстави стверджувати про особливу актуальність процесів пошуку, збирання і добування інформації у відкритих, відносно відкритих і закритих електронних джерелах; заходів із забезпечення конфіденційності, цілісності та доступності власного ІР, а також протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз. Зважаючи на це і враховуючи постійно зростаючий потенціал використання мережі Інтернет у військових цілях, провідні країни світу (США, Японія, Франція, Велика Британія, Росія, Китай, Ізраїль та багато інших) протягом останніх років активно модернізують власні безпекові простори і кібернетичну безпеку, відводячи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази.

У практику збройної боротьби вони активно впроваджують концепцію інформаційного протиборства, яка передбачає ведення активних розвідувальних дій щодо об'єкта нападу або потенційного порушника та дій, спрямованих на захист національних інтересів від впливу внутрішніх і зовнішніх кібернетичних загроз і небезпек.

Наслідком таких дій невдовзі можуть стати так звані кібернетичні війни, основними методами ведення яких на тактичному рівні вже нині визнані кібератаки, а на стратегічному і спеціальному рівнях – кібероперації та кіберкампанії. Практично всі вони в умовах сьогодення досягають очікуваного від них результату.

Підтвердженням цьому є такі атаки:

– 12 травня 2017 р. тисячі комп'ютерів в усьому світу зазнали масованої атаки хакерів, які розповсюдили програму-здирника WannaCry. За даними лабораторії Касперського, було зафіксовано 45 тисяч спроб зараження програмою-шифрувальником у 74 країнах світу (https://toneto.net/news/kultura/ssha-gotovi-pomoch-miru-borotsya-s-kiberatakami);

– атаки, спричинені вірусами Stuxnet і Hydraq – двома найпомітнішими кіберподіями 2010 р.;

– атаки, спричинені троянськими вірусними програмами Duqu і Flame (2011 р.), Mahdi та Gauss (2012 р.);

– події навколо сайту Wikileaks, які кардинально змінили межі загроз і показали всьому світу, що можливості кіберзброї можуть бути досить вражаючими, а протидія її негативному впливу може виявитися вкрай складним завданням для сторін, що захищаються.

Такий стан справ дає підстави стверджувати, що відсутність надійної *системи забезпечення кібернетичної безпеки* може призвести до втрати політичної незалежності будь-якою державою світу, тобто до фактичного програшу нею війни невійськовими засобами і підпорядкування її національних інтересів інтересам іншої (протиборчої) сторони [7, с. 5–6].

Оскільки система забезпечення кібербезпеки України є на етапі становлення, із суто теоретичних міркувань постає потреба у з'ясуванні ключових концептів понятійно-категорійного ряду.

Насамперед акцентуємо увагу на відсутності уніфікованої дефініції системи забезпечення кібербезпеки. Тому пропонуємо сформулювати авторське розуміння шляхом адаптації подібних, наприклад, найближчою за суттю є визначення системи забезпечення національної безпеки.

Із різноманіття запропонованих дефініцій наведемо ті, що, на нашу думку, є найбільш вдалими.

Система забезпечення національної безпеки – це «організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями і завданнями щодо захисту національних інтересів, які здійснюють узгоджену діяльність у межах законодавства України» [2, с. 317].

Система – це «сукупність об'єктів і відносин між ними, що у своїй органічній єдності утворюють нову якість» [2, с. 314].

Система забезпечення безпеки – це «сукупність організаційно об'єднаних органів управління, сил і засобів, призначених для вирішення завдань щодо забезпечення національної безпеки» [2, с. 315].

Кібербезпека – це «стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз функціонуванню його елементів» [4, с. 188].

Кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їхній сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам. Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо IP, ІКТ і ІТС [6, с. 15].

Окремо схематично зазначимо про складові частини кібернетичної безпеки.

Підтримуємо положення про те, що забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі досягається комплексним застосуванням сукупності правових, організаційних, інформаційних та заходів стратегічних комунікацій [9].

Об'єднавши вищезазначені дефініції, сформулюємо авторське розуміння системи забезпечення кібербезпеки як сукупності організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на захист кіберпростору від атак, а також сил, засобів і методів, які використовуються для досягнення цілі у межах законодавства України.

Оскільки поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства у мережі Інтернет, кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави, то нагальним є створення національної системи забезпечення кібербезпеки як складової частини системи забезпечення національної безпеки України [9].

Сформулювавши поняття системи забезпечення кібербезпеки, визначимо її зміст, тобто сутність та особливості.

Завдання системи безпеки – створити такі умови, за яких, досягаючи належного рівня формування достатніх і необхідних умов для реалізації національних інтересів і цілей, члени системи водночас реалізовували б свої індивідуальні цілі та завдання [2, с. 388], а отже, завданням системи забезпечення кібербезпеки є формування ефективно функціонуючого механізму створення необхідних умов у кіберпросторі, за яких уможливлюється реалізації національних інтересів у кібернетичній сфері.

У Стратегії кібербезпеки прямо зазначено, що основу національної системи забезпечення 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, на які мають бути покладені в установленому порядку відповідні завдання [9]. Незрозумілим є невключення Верховної Ради України до цього переліку, оскільки вона є єдиним законодавчим органом, а тому відіграє важливу роль у забезпеченні кібербезпеки.

Окремо зазначимо про Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України. Основними завданнями Центру є такі: здійснення аналізу стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань із питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо [10].

Реальна ситуація, що склалась у сфері кібербезпеки України, є такою: кібернетичні атаки на

інформаційні ресурси держави стали невід'ємним компонентом гібридної війни проти України, що її розв'язала Росія.

Таким чином, проблема зростання кіберзагроз стає вкрай актуальною та для свого розв'язання потребує ефективних заходів з оптимізації системи кібербезпеки держави. Не можна не відзначити, що всі спроби змін і реформування моделі забезпечення кібербезпеки держави здійснюються в умовах майже цілковитої закритості даних про стан суспільних відносин у сфері кібербезпеки, реальні показники захисту об'єктів критичної інфраструктури від кібератак.

Навіть з урахуванням особливостей втаємничення процесів планування у сфері національної безпеки, ступінь закритості в кібербезпековій сфері залишається надзвичайно високим, що значно зменшує повноцінну можливість участі інститутів громадянського суспільства у забезпеченні кіберебзпеки. Стан закритості спостерігається не лише щодо інформування суспільства і фахівців, а й для самих суб'єктів забезпечення кібербезпеки держави. Держава часто опиняється у стані, коли достеменно не знає, яким ресурсом володіє і які можливості мають її органи. Це унеможливлює побудову справді цілісної та ефективної системи забезпечення кібербезпеки держави, що складається як із захисних, так і з наступальних систем та засобів.

Окремі дані щодо стану кібербезпеки держави оприлюднюються лише CERT-UA, а в деяких випадках – СБУ і МВС (у вигляді повідомлень про затримання тих чи інших зловмисників). Інша статистична інформація майже відсутня або надається за окремими запитами. Можна констатувати, що до останнього часу проблеми у сфері кібербезпеки, а також пошук шляхів їх вирішення базувалися не на цілісному та методологічно правильно проведеному огляді стану та проблем сфери, а більшою мірою на суб'єктивному сприйнятті окремими фахівцями і дослідниками сфери кібербезпеки України її стану та перспектив.

При цьому, якщо Україна, як і більшість держав світу, фактично визнає кіберпростір рівноправним простором суперництва (зокрема, військового), то до планування діяльності держави в ньому доцільно застосовувати ті ж підходи, що і до військової сфери та взагалі сфери державного управління. Усе це зумовлює необхідність проведення комплексного огляду сфери кібербезпеки України, який із залученням усіх зацікавлених сторін має дати відповіді на такі питання:

– актуальний дереват національних інтересів у кібернетичній сфері з виокремленням пріоритетних;

– національні цінності України як базовий концепт формування національних, зокрема життєво важливих, інтересів у кібернетичній сфері;

– формування засад національної ідентичності в умовах ведення гібридної війни та формування суперницьких відносин у кіберпросторі, спрямованих на зміну генетичного коду нації;

– стан і прогнозований розвиток за певно визначеними індикативними показниками суспільних відносин у кібернетичній сфері;

– ресурсний та інший потенціал системи забезпечення кібербезпеки;

– напрями державної політики у сфері кібербезпеки;

– співвідношення зазначеного вище із Законом України «Про основи національної безпеки України», Стратегією національної безпеки України, Доктриною інформаційної безпеки і Стратегією кібербезпеки України.

Важливою особливістю кіберпростору є його висока динамічність і мінливість загроз. Це зумовлює неможливість створення Стратегій, які охопили б періоди більші, ніж три – п'ять років (а реально – до двох). Відповідно, щонайменше кожні два роки Стратегія кібербезпеки України буде потребувати корегування відповідно до нових викликів і загроз, а також змін у геополітичному безпековому середовищі [8].

Незважаючи на прийняття Стратегії кібербезпеки України, система забезпечення кібербезпеки потребує активних дій, а вони, у свою чергу, вимагають значної кількості ресурсів як фінансового, так і технічного характеру, а також людського потенціалу, інформаційної грамотності та інформаційної освіти.

Також акцентуємо увагу на тому, що система забезпечення кібербезпеки не може бути ізольованою від усієї міжнародної спільноти, а тому важливою є співпраця з іншими державами та міжнародними організаціями задля максимально ефективного її функціонування. Зокрема, актуальним є вивчення зарубіжного досвіду з метою запозичення позитивних здобутків та адаптації цих норм у національне законодавство, а також урахування стандартів ЄС і НАТО з метою створення підґрунтя для реалізації національних інтересів.

Окремої ваги набуває поінформованість населення про кіберпростір загалом і систему забезпечення кібербезпеки зокрема з метою можливості його залучення до виконання різноманітних завдань, а також виявлення, запобігання та нейтралізації кіберзагроз. Як зазначено в Конвенції про кіберзлочинність, ефективна боротьба з кіберзлочинністю вимагає більшого, швидкого й ефективно функціонуючого міжнародного співробітництва у кримінальних питаннях [11], однак вона, по-перше, присвячена доволі вузькому сегменту кіберзагроз (кіберзлочинам у сфері комп'ютерної інформації), а по-друге, по суті, є регіональним документом, який не сприймається значною кількістю геополітичних акторів.

Сторони Конвенції (Україна є учасником. – Авт.) співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів в електронній формі, які стосуються кримінальних правопорушень [11].

Важливим напрямом правового забезпечення системи кібернетичної безпеки України є також поглиблення міжнародного співробітництва у цій сфері. З огляду на те, що жодна держава неспроможна самостійно забезпечити ефективний захист об'єктів національної інфраструктури у кіберпросторі, такі системи розроблюються кожною із провідних держав світу з урахуванням принципів міжнародного співробітництва та перспективами їх інтеграції у глобальну систему кібербезпеки. Враховуючи міжнародний досвід, до основних заходів правового забезпечення кібернетичної безпеки України варто віднести:

– впровадження законодавчих механізмів щодо отримання правоохоронними органами України інформаційної, консультативної та технічної допомоги від приватного сектору (операторів і провайдерів зв'язку, виробників комп'ютерної техніки, розробників програмного забезпечення тощо);

– формування правової основи конструктивного міжнародного співробітництва з якомога ширшим колом компетентних органів інших країн щодо оперативного обміну інформації про інциденти у кіберпросторі та проведення спільних правоохоронних заходів;

– забезпечення подальшого розвитку правових основ міжнародного співробітництва з протидії кіберзагрозам, зокрема шляхом налагодження співпраці зі Спільним центром передового досвіду з кіберзахисту (м. Таллінн, Естонська Республіка), з метою обміну досвідом і проведення спільних заходів [6, с. 319].

Також підтримуємо норму про те, що розвиток і безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими частинами державної політики у сфері розвитку інформаційного простору і становлення інформаційного суспільства в Україні [9].

Окремо зауважимо про те, що забезпечення безпеки існування і функціонування інформаційних ресурсів фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій повинно бути одним із головних завдань діяльності аналізованої нами системи.

Як зазначено у Стратегії [9], недостатня ефективність суб'єктів системи забезпечення національної безпеки України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру, а також недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки є чинниками, через дію яких актуалізуються загрози кібербезпеці.

У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки як найбільш оптимальні організаційні структури, що здатні в короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам. В Україні також відбувається процес формування системи кібернетичної безпеки. Як складову частину такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 р. доручалося розробити Кабінету Міністрів України за участю Служби безпеки України. Водночас недосконалість національного законодавства у сфері забезпечення кібернетичної безпеки значно підвищує імовірність реалізації таких загроз, що негативно впливає на загальний рівень національної безпеки України [6, с. 312].

Недоліки понятійного апарата у сфері забезпечення кібернетичної безпеки не дозволяють:

– визначити ознаки й об'єктивно оцінити основні загрози у національному сегменті кіберпростору;

– визначити найбільш ефективні заходи забезпечення кібернетичної безпеки;

– чітко сформулювати завдання і функції суб'єктів кібернетичної безпеки тощо.

У законодавстві відсутнє визначення не лише поняття «кібернетична безпека» (кібербезпека), а й таких понять, як «кібернетичний простір» (кіберпростір), «кібернетична загроза» (кіберзагроза), «кібернетична атака» (кібератака), «кібернетичний захист» (кіберзахист), «кібернетичний злочин» (кіберзлочин), «кіберзлочинність», «кіберінцидент» тощо [6, с. 313].

Водночас теоретико-методологічні дискусії довкола термінологічної бази стикаються зі значно більш практичною проблемою – застосування чинного нормативно-правового поля (особливо міжнародного) щодо кіберзагроз і з'ясування самої можливості його застосування у відповідному контексті. Особливо важливо вирішити кілька принципових ускладнень, що унеможливлюють формалізацію безпекової політики в кіберпросторі: досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростору та всім його «безпековим» похідним; не визначено правовий статус кіберпростору; на міжнародному рівні відсутній консенсус щодо правил поведінки в кіберпросторі; відсутні загальноприйняті методології оцінки наслідків кіберзлочинів та їх розгляду як об'єкта міжнародних норм і правил (зокрема, щодо визнання кібератаки актом війни). Незважаючи на широкий інтерес до зазначеного безпекового напряму, наукові дослідження (чи навіть узагальнення із цього питання) досі є поодинокими й часто несистемними [1].

Кібернетична безпека України гарантується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм [6, с. 314], а система її забезпечення повинна існувати у їхніх межах.

Існує думка, що базовий закон, який має визначати основні засади державної політики щодо забезпечення безпеки людини і громадянина, суспільства та держави від зовнішніх і внутрішніх загроз у кібернетичному просторі, доцільно назвати «Про основи

кібернетичної безпеки». Цим законом повинні регулюватись як відносини захисту від кіберзагроз, так і відносини, пов'язані з нейтралізацією джерел таких загроз (це, насамперед, протидія кіберзлочинам та іншим правопорушенням у цій сфері) [6, с. 315]. Але, на наш погляд, тиражування законів не є оптимальним і правильним шляхом регулювання суспільних відносин у цій сфері. Адже в Україні вже існує доволі значна кількість нормативно-правових актів, що регулюють суспільні відносини у цій сфері, зокрема ухвалено Стратегію кібербезпеки, тому, на нашу думку, цього абсолютно достатньо для реалізації державної кібербезпекової політики. Водночас, не підтримуючи ідею формування окремого закону, хотіли б висловити свою позицію щодо необхідності розроблення і прийняття Концепції державної інформаційної політики, в рамках якої на підставах Закону України «Про основи національної безпеки України», Стратегії національної безпеки України, Доктрини інформаційної безпеки України, Стратегії кібербезпеки України наша держава змушена у стислі строки сформувати цілісну і тверду позицію щодо забезпечення кібербезпеки власного кіберпростору, який нині є полем нового геополітичного протистояння. Саме тому діяльність щодо кіберпростору повинна бути спрямована на пошук напрямів підвищення кібербезпеки держави, функціонування якої регулюється системою публічного управління.

Зусилля основних світових гравців перебувають у протилежних векторах розвитку кіберпростору: з одного боку, офіційні зусилля спрямовані на демілітаризацію кіберпростору і недопущення перетворення його на нове поле збройного протистояння, а з іншого – де-факто триває процес протистояння. В умовах невизначеності кібербезпекової політики України та з урахуванням її перебування на перетині інтересів основних геополітичних гравців такий стан речей зумовлює необхідність якнайшвидшої розбудови всіх основних секторів держави за напрямом забезпечення кібербезпеки [1].

Вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру та масштабам реальних і потенційних кіберзагроз життєво важливим інтересам людини і громадянина, суспільства і держави. З метою забезпечення належного рівня кібернетичної безпеки повинні бути сформовані:

– загальнодержавна система протидії кіберзлочинності та кібертероризму як сукупність спеціальних суб'єктів протидії кіберзлочинності і кібертероризму, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних і технічних заходів, що ними здійснюються;

– загальнодержавна система кібернетичного захисту об'єктів національної критичної інфраструктури як сукупність спеціальних суб'єктів забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних і технічних заходів [6, с. 318].

Україна продовжує спроби створення повноцінної системи національної кібербезпеки. Основним механізмом обрано унормування профільним законом і Стратегією кібербезпеки України. Це відбувається на тлі активності РФ у кіберпросторі, що має усі ознаки антиукраїнської та переслідує отримання непублічних відомостей та атаки на сайти органів державної влади [8].

Крім проблем нормативно-правового характеру, доводиться констатувати брак міжвідомчої координації із питань забезпечення кібербезпеки держави. Нині в Україні відсутні загальнонаціональні міжвідомчі координаційні структури, 13 спроможні узгоджувати й координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі та створення ефективної системи захисту вітчизняного кіберпростору.

Координування із питань забезпечення кібербезпеки держави має відбуватися на двох рівнях – стратегічному й оперативному.

Стратегічне координування є зоною відповідальності Ради національної безпеки і оборони України, а оперативне (з урахуванням підпорядкованості безпекових структур) доцільно здійснювати силами Національного центру кібербезпеки при Президентові України, який слід створити у найкоротший термін. Невиконання цієї вимоги матиме результатом небажання окремих суб'єктів забезпечення безпеки співпрацювати з іншими уповноваженими відомствами через законодавчу (нормативну) невизначеність прав та обов'язків цих структур чи невідповідність певних нормативних документів вимогам часу.

Ця ситуація уже має місце, а в тих випадках, коли така співпраця існує, найчастіше вона здійснюється на рівні міжособистісних зв'язків керівників відповідних підрозділів. Із погляду довгострокової перспективи така ситуація є прямою загрозою кібербезпеці держави. При цьому профільні науково-дослідні інститути, задіяні в комплексних дослідженнях кібербезпеки, майже відсутні. Ще одна проблема полягає у тому, що Україна (особливо телекомунікаційний компонент її інформаційної інфраструктури) й досі є принципово вразливою до кіберзагроз і не в останню чергу через надміру широке транслювання іноземних програмних продуктів і використання матеріально-технічної бази іноземного виробництва. Пошук можливих «закладок» у цій продукції практично унеможливлюється через залежність Української держави від згаданих продуктів, що вийшла на справді загрозливий для національної безпеки рівень в усіх сферах [1].

Україна як самодостатня і суверенна держава з часу здобуття незалежності шляхом налагодження співробітництва з міжнародними інституціями прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору. Проте, як зазначають вітчизняні й західні фахівці, нині існує ціла низка проблем, що заважають нашій державі це зробити.

До найбільш значущих серед них слід віднести:

– деградацію науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інформаційній сфері та низький рівень конкурентоспроможності в ній;

– значну вразливість інформаційної сфери України через надмірно широке впровадження у ній західних програмних продуктів (зокрема, фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва;

– непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту, їхнє незадовільне кадрове забезпечення відповідними кваліфікованими фахівцями;

– відсутність загальнонаціонального координаційного центру, спроможного узгоджувати й координувати діяльність зазначених вище правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпросторам України, керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави в інформаційній сфері на кшталт "Cyber Storm", які проводяться у США, та/або "Cyber Europe", що проводяться у ЄС;

– відсутність єдиного понятійно-термінологічного поля кібербезпеки України як головного складника інформаційної безпеки, а також системних нормативно-правових документів, які б регламентували діяльність зазначених відомств, правоохоронних і силових структур у сфері кіберзахисту, тощо [7, с. 8].

Таким чином, у результаті проведеного дослідження резюмуємо таке.

Під системою забезпечення кібербезпеки варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на реалізацію національних інтересів у кібернетичній сфері, а також сил, засобів і методів, які використовуються для досягнення цілі відповідно до законодавства України. Завданням системи забезпечення кібербезпеки є створення необхідних умов у кіберпросторі, за яких можливим є досягнення загальнодержавних цілей і реалізація інтересів, завдань та цілей її елементів.

Незрозумілим є невключення Верховної Ради України до переліку суб'єктів, які становлять основу національної системи забезпечення кібербезпеки. Об'єктом системи забезпечення кібербезпеки і є сама кібербезпека. Побудова дієвої системи забезпечення кібернетичної безпеки України вимагає коректного і точного визначення державної політики у цій сфері, випереджального правового реагування на динамічні зміни, що відбуваються у кіберпросторі.

ЛІТЕРАТУРА:

1. Черноног О.О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління / О.О. Черноног [Електронний ресурс]. – Режим доступу : mino.esrae.ru.

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

3. Ліпкан В.А. Поняття системи забезпечення національної безпеки України / В.А. Ліпкан // Право і Безпека. –2003. – Т. 2. – № 4. – С. 57–60.

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

5. 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/.

6. 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.

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

8. Питання створення «Огляду сектору кібербезпеки України». Аналітична записка [Електронний ресурс]. — Режим доступу : http://www.niss.gov.ua/articles/1911/.

9. Стратегія кібербезпеки України від 15.03.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016.

10. Порошенко підписав указ про Національний координаційний центр кібербезпеки, 08.06.2016 р. [Електронний ресурс]. – Режим доступу : http://ua.censor.net.ua/n392282.

11. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/994_575.