УДК 355.451:004.7

Г. Дзяна,
Н. Дзяний

РЕАЛІЗАЦІЯ НАЦІОНАЛЬНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

Розкрито особливості реалізації національної політики у сфері кібербезпеки. Проведено аналіз кібератак на інфраструктурні об'єкти України. Визначено проблемні питання забезпечення кібербезпеки інфраструктурних об'єктів. Деталізовано напрями вдосконалення національної політики забезпечення кібербезпеки.

Ключові слова: інформаційний простір, інформаційна безпека, кіберпростір, кібербезпека, кібератаки, кіберзахист інфраструктурних об'єктів.

Протягом останніх років виникла стійка тенденція до збільшення проявів комп'ютерних атак на важливі об'єкти інфраструктури різних держав, що призводило до завдання їм шкоди через спотворення важливої інформації, блокування виробничих процесів на об'єктах промисловості, житлово-комунального господарства, транспорту, енергетики.

Стрімкий розвиток в Україні інформаційних технологій та інтеграція України до світового інформаційного простору створюють передумови для реалізації аналогічних кіберзагроз щодо вітчизняної інфраструктури. Зазначене потребує вжиття на державному рівні комплексу організаційних, правових, наукових, технічних заходів та вимагає поглибленого наукового дослідження, оскільки в майбутньому важливість кібербезпеки тільки зростатиме.

Дослідження проблем забезпечення інформаційної та кібернетичної безпеки держави у своїх працях розглядали: В. Панченко, В. Петрик, В. Ліпкан, В. Бурячок, О. Баранов, С. Гнатюк, Д. Дубов, О. Корченко, В. Номоконов, В. Петров, В. Тулупов, В. Шеломенцев. Питанням захисту критичної інфраструктури, методології ідентифікації об'єктів критичної інфраструктури присвячено роботи Д. Бірюкова, С. Кондратова, С. Гнатюка, В. Лядовської та інших.

Праці цих науковців та фахівців-практиків створили методологічне підґрунтя для системного дослідження багатьох проблем у сфері забезпечення інформаційної та кібербезпеки України. Проте подальшого комплексного вивчення потребує питання удосконалення національної політики у сфері забезпечення кібербезпеки.

Метою статті є узагальнення основних положень реалізації національної політики у сфері забезпечення кібербезпеки.

Поширення новітніх інформаційно-комунікаційних технологій та стрімкий розвиток інформаційно-телекомунікаційних систем призвели до формування *інформаційного суспільства*, а також *інформаційного* та *кібернетичного просторів*, які мають на сьогодні практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни. В умовах розвитку інформаційного суспільства інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки.

На сьогодні, на рубежі тисячоліть, сформувалося поняття *інформаційного простору* як глобального інформаційного середовища, яке в реальному масштабі часу

забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення з метою підтримання ухвалюваних рішень щодо створення оптимального, задля досягнення поставлених цілей, складу сил і засобів та їх ефективного застосування в різних умовах навколишньої обстановки.

Інформаційну безпеку у найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони [1]. Досягненню успіху у виконанні завдань у різних сферах суспільного життя значною мірою сприятиме проведення ефективної національної інформаційної політики та забезпечення інформаційної безпеки держави.

Інформаційна інфраструктура держави – це сукупність носіїв даних та інформації суб'єктів інформаційної діяльності держави, які реалізовані у формі організаційно-технічних засобів (інформаційних систем, центрів та пунктів, засобів масової інформації), що здійснюють створення, накопичення, зберігання, обробку і поширення інформації, засобів захисту інформації, а також організаційних структур, які забезпечують їх функціонування згідно із чинним законодавством.

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело, зрештою, до формування кіберпростору. Відповідно до офіційних документів Євросоюзу, *кіберпростір* – це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів. Відповідно до офіційних документів Німеччини, *кіберпростір* – це вся інформаційна інфраструктура, доступна через Інтернет поза будь-якими територіальними кордонами [2].

Кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам (рис. 1.) [3].

Рис. 1. Складові кібернетичної безпеки

Непростий стан справ у сучасному інформаційному суспільстві зумовлює небачені досі глибинні зміни у ставленні більшості держав світу до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її обробки та кіберсередовища, в якому ця інформація циркулює (рис. 2.), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки [4].

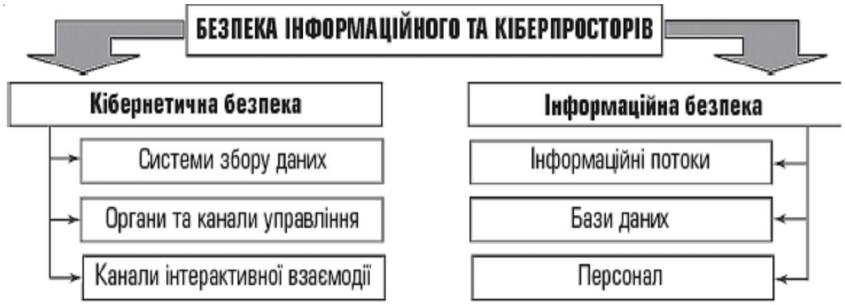

Рис. 2. Об'єкти впливу в інформаційному та кіберпросторі

Кіберпростір на сьогодні можна розглядати як середовище обробки інформації державного та корпоративного призначення, що є деякою віртуальною сутністю, яка не має конкретної матеріальної форми, але проявляється в об'єктивності взаємодії людей і організацій у мережі Інтернет, а також асоційованого з ним технологічного обладнання та мереж. Безпекою кіберпростору або кібербезпека – це безпека цієї віртуальної сутності, цього віртуального світового інформаційного простору. Кібербезпека, своєю чергою, ґрунтується на таких компонентах (рис. 3) [5]:

Рис. 3. Місце кібербезпеки згідно з ISO 27032

– інформаційна безпека – це заходи забезпечення конфіденційності, цілісності та доступності інформації для задоволення потреб користувачів;

– безпека застосунків – це менеджування ризиків, що застосовується не тільки до самих додатків (їх процесів, компонентів, програмного забезпечення та результатів), але і до даних (даних конфігурації, користувальницьких даних, організаційних даних), а також і до всіх технологій, активностей та акторів, залучених у життєвий цикл додатка;

– безпека мереж – це технічний стан мережі, що досягається в процесі її розробки, створення, функціонування і модернізації та гарантує конфіденційність, цілісність і доступність інформації користувачів цієї мережі;

– безпека роботи в мережі Інтернет розглядається як розширення поняття мережевої безпеки шляхом включення до нього захищених Інтернет-залежних сервісів, систем і мереж;

– захист інформації в критичних системах інформаційної інфраструктури розглядається в контексті критично важливих секторів; захист критичної інформаційної інфраструктури передбачає забезпечення гарантії того, що подібні системи та мережі стійкі відносно ризиків інформаційної безпеки, мережевої безпеки, безпеки Інтернет, так само як і ризиків кібербезпеки.

На цей час значна частина кібератак в кіберпросторі здійснюється з використанням найпоширенішого шкідливого програмного забезпечення, такого як [6]:

– класичні комп'ютерні віруси;

– мережні черв'яки;

– "троянські коні";

– спеціальні засоби (експлойти, генератори ключів тощо).

Кібератаки можна розділити на такі основні групи: напад зсередини приватної мережі, напад зовні приватної мережі та їх комбінації. Організація механізму реалізації і просування кібератак може відбуватися на основі сумнівних веб-сайтів, неконтрольованих завантажень, розсилки спаму, віддаленого управління або заражених вірусами знімних носіїв.

Стан захищеності українського кіберпростору різко погіршився упродовж останніх трьох років. У 2014 р. Україна посіла 5 місце в рейтингу країн, на які здійснюються кібератаки. Такі результати дослідження кіберзагроз, проведеного фахівцями "Kaspersky Lab" у третьому кварталі 2014 р. Однак, за даними американської компанії, станом на квітень 2015 р. Україна і США очолили список жертв шпигунських кібератак. Компанія щорічно проводить дослідження, використовуючи дані міжнародних партнерів у сфері комунікацій, а також, дані секретної служби США і департаменту національної безпеки США. За даними американської компанії, минулого року список жертв шпигунських кібератак очолили Україна і США. За їхніми розрахунками, в публічному секторі у 2015 р. було здійснено 120 атак, у 40% випадків їх жертвами стали Україна та США [7].

Українсько-російське протистояння – приклад активнодіючого кібертероризму, оскільки за останні три роки Україна витримала велику кількість сфокусованих на неї кібератак. Фахівці з кібербезпеки і захисту даних зазначають, що аналіз таких подій, як Євромайдан, окупація Криму, війна РФ проти України показав, що найважливішими невирішеними проблемами в сфері кібербезпеки є незахищеність критичної інфраструктури, причому не тільки кібератак, а й фізичних атак. Також відзначено високу кількість заражених вірусами і неправильно сконфігурованих систем в українському сегменті Інтернету.

Протягом 2013 – 2016 рр. в Україні діють як внутрішні кіберорганізації (наприклад, "КіберБеркут"), так і зовнішні (кібератака з боку Росії). Хакерська група "КіберБеркут" – Інтернет-бренд, під яким відбуваються хакерські атаки, здебільшого на сайти державних і громадських організацій України. Хто керує брендом – невідомо. Американський спеціаліст з комп'ютерної безпеки Дж. Карр вважає, що це група проросійських хактивістів. Група офіційно оголосила свої цілі: боротьба з неофашизмом, націоналізмом і свавіллям влади в Україні. Саме "КіберБеркут" взяв на себе відповідальність за порушення роботи системи електронного підрахунку голосів на парламентських виборах. Окрім того, на рахунку хакерської організації такі кібератаки: опублікування листування народних депутатів, блокування телефонів стільникового зв'язку членів чинного уряду України, тимчасове блокування роботи сайтів МВС України та Генеральної прокуратури України, тимчасове блокування роботи сайтів телеканалів "Інтер" і "1+1" [8].

Іншою активною хакерською організацією, що здійснює кібератаки на Україну, є "Анонімус" – сучасна вільно організована група хактивістів. Термін з'явився у 2003 р. як концепція великої кількості онлайн- і оффлайн-співтовариств користувачів, що представляють собою анархічний цифровий світовий розум. Починаючи з 2008 р., "Анонімус" починає поставати як міжнародний хактівізм. Велику кількість кібератак організація здійснила відносно України. Найвідоміші кіберзломи: злам електронної пошти МЗС України; злам серверів української митниці; злам електронної пошти депутатів тощо. Найбільш значна частина кібертерористичних атак на Україну здійснювалася з боку Росії. Американське видання "Fortune" у своїй статті висуває припущення, що активність російських кібератак підвищується, як тільки в Україні готується військова операція [9].

У звіті фірми "Lookingglass", що займається кібербезпекою, йдеться про кіберкампанії, які ведуться російською стороною проти українських об'єктів, таких як уряд, правоохоронні та військові органи. Мета подібного шпигунства – зібрати розвідувальні дані про противника і підтримати російські військові зусилля. Згідно з доповіддю, кіберкампанії стартували в середині 2013 р. Після оголошення початку антитерористичної операції в Україні в середині квітня 2014 р. кількість кібератак значно збільшилася [10]. За даними Lookingglass, з цього моменту російські кібератаки були безпосередньо пов'язані з датами військових подій, а їх метою став збір розвідувальної інформації, щоб розширити свої можливості на полі бою. Останні звіти свідчать про те, що російські шпигуни проникли глибоко всередину розвідувального апарату України.

Вважається, що повномасштабна кібервійна Росії проти України розпочалася в березні 2014 р. із моменту, коли Росія запустила в мережу вірус "Змія", який надає повний доступ до атакованої системи [11]. Кібератаки здійснювані Росією проти України направлені на те, щоб дістати якомога більше інформації із державних структур. Для того, щоб протистояти цим атакам, українські активісти створили в Інтернеті кілька спільнот, які займаються пошуком і блокуванням електронних рахунків лідерів так званих "народних республік" на Донбасі і навіть блокуванням номерів їхніх мобільних телефонів.

Окрім того, українські спецслужби розслідують кібератаки, які обрушились на Україну наприкінці минулого року. Напади стались відразу на чотири обленерго: "Прикарпаттяобленерго", "Київобленерго", "Чернівціобленерго" та "Хмельницькобленерго". Результат – знеструмлення помешкань сотень тисяч українців. Хакери й далі продовжують цілитися в стратегічно важливі об'єкти, тому влада запевняє, що посилює боротьбу з ними – у березні Президент України П. Порошенко затвердив Стратегію кібербезпеки України.

Це була перша атака з такими негативними наслідками: кібертерористи одночасно вимкнули кілька десятків високовольтних вимикачів на підстанціях чотирьох обленерго. Ця аварія – попереджувальний постріл. Подальший розвиток подій залежав від адекватності сприйняття рівня загрози всіх без виключення керівників стратегічних підприємств і держави. Зазвичай хакерські атаки компаній та державних установ націлені на оволодіння доступом до комерційної інформації з метою нанесення прямих збитків конкурентам або для отримання матеріальної здобичі шляхом пограбування через мережі. Але найбільшу загрозу, а відтак і стурбованість людей, спричиняють заплановані терористичні акти в аеропортах, на атомних електростанціях, залізничних вокзалах та інших стратегічних об'єктах [12].

Хакери перебирають на себе управління інформаційними системами чи технологічними процесами підприємств, а виявити інстальовані комп'ютерні віруси не

завжди вдається з допомогою існуючих засобів захисту. Наслідки можуть бути катастрофічними не лише для бізнесу, але й для життя багатьох людей.

За повідомленням СБУ, після розслідування кібератак на "Прикарпаттяобленерго", "Київобленерго", "Чернівціобленерго" та "Хмельницькобленерго" з залученням міжнародних експертів з кібербезпеки було виявлено шкідливе програмне забезпечення типу BlackEnergy в мережах цих компаній.

У всіх вказаних випадках встановлено віддалений несанкціонований доступ з території РФ, із застосуванням BlackEnergy до систем телеметрії та телефонного зв'язку вищезгаданих підприємств. В ході розслідувань встановлено, що задовго до кібератаки хакери почали розсилати до українських обленерго листи, в яких були документи Microsoft Word. Коли їх відкривали, на комп'ютер одержувача інсталювалися шкідливі програми, унаслідок активації яких у систему встановлювалася троянська програма Backdoor.Fonten.Win32.4. Троян містив шпигунський модуль, який збирав інформацію про систему і мережі, та відправляв її на віддалений командний центр, підконтрольний зловмисникам, що дало змогу зібрати логіни та паролі, за допомогою яких комп'ютерні терористи отримали можливість здійснити атаку [13].

Так був одержаний доступ у режимі реального часу до управління телекомунікаційними мережами, чим і скористалися хакери для організації Як наслідок проведених кібератак, було виведено з ладу кілька серверів і робочих станцій, що вплинуло на їх роботу та ускладнило відновлення діяльності енергосистем.

Доцільно зазначити, що після подій в Україні про небезпеку подібних кібератак заявили США, Велика Британія, Норвегія, Німеччина та інші країни. Світова спільнота занепокоєна збільшенням кількості кібератак на об'єкти критичної інфраструктури та закликає шляхом об'єднання зусиль різних країн протистояти потенційній загрозі.

Проблеми в кіберпросторі були викликані тим, що держава і бізнес, на думку експертів, діють недостатньо ефективно проти кіберзагроз. І хоча великі корпоративні компанії приділяють увагу захисту даних і виділяють певні ресурси на ці цілі, існує низка проблем: по-перше, практично відсутній процес обміну деталями кібератак; по-друге, швидкість реагування на кіберзагрози досить низька, наприклад, відомі факти, коли кіберзлочинці тижнями скачували дані з серверів українських компаній вже після оприлюдненої інформації про знаходження уразливості в програмі шифрування; по-третє, відсутня масова практика обміну шифрованими повідомленнями електронної пошти. У державному секторі існуюча система стандартів у галузі безпеки застаріла, відірвана від бізнес-практик, не гарантує фінансово обґрунтованих і надійних заходів захисту. Усе ще чи не повсюдно використовується піратське програмне забезпечення, програми виробництва РФ або нелегальних російських хакерських груп. Фахівці в державних органах не завжди мають достатні компетенції для реалізації заходів із кібербезпеки, відсутня належна координація дій між різними державними підрозділами відповідної спеціалізації [14].

З огляду на те, що кібератаки значно почастішали, українська влада вирішила посилити механізми захисту державних комп'ютерних систем. 16 березня 2016 р. Президент України видав Указ про введення в дію рішення Ради національної безпеки та оборони України "Про Стратегію кібербезпеки України" від 27.01.2016 р. [15]. У концептуальному документі визначено ворожу сторону, яка веде розвідувально-підривну діяльність у кіберпросторі. Цьому сприяє широка, інколи домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, прямо чи опосередковано пов'язаних із Російською Федерацією.

Таким чином, з зазначеного вище випливає, що в Україні стартував етап практичного втілення на державному рівні технологій кібербезпеки. На виконання зобов'язань Президента, Кабінет міністрів спільно з СБУ, Службою зовнішньої розвідки за участі Інституту стратегічних досліджень повинні розробляти щорічні плани заходів щодо реалізації Стратегії кібербезпеки України. Окрім того, в складі Ради національної безпеки і оборони України вже створено робочий орган – Національний координаційний центр кібербезпеки, поява якого на сьогодні є цілком обґрунтованою. Адже повсюдне використання інформаційних технологій призвело і до їх активного використання для здійснення терористичних актів та кібератак на важливі об'єкти критичної інфраструктури.

Висновки

На сьогодні кіберпростір став територією активного протистояння. Сучасні комп'ютерні системи є вразливими. Кібератаки здійснюються за допомогою спеціально розробленого програмного забезпечення, що використовує вразливості комп'ютерних систем. Виявлення таких атак ускладнюється тим, що вони здійснюються на обмежену кількість спеціально визначених цілей, не викликають збоїв і відмов комп'ютерів, а тому тривалий час не потрапляють у поле зору дослідників із антивірусних лабораторій. Методи захисту не завжди ефективні і вимагають розвитку.

Очевидно, що ефективний кіберзахист інфраструктурних об'єктів має бути пріоритетом державної політики, оскільки розвиток кіберпростору призвів до змін у підвищенні ступеня взаємозв'язку, взаємопроникнення і взаємозалежності різноманітних мереж і систем, виробничих, фінансових, торговельних та інших процесів у всіх сферах життя більшості країн світу, забезпечення суверенітету України та її обороноздатності з огляду сталого розвитку держави на довгострокову перспективу.

Отже, пошук шляхів підвищення ефективності кібербезпеки інфраструктурних об'єктів держави потребує дослідження нової "гібридної" безпеки реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні безпеки держави і вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки інфраструктурних об'єктів. Найефективнішим шляхом вирішення зазначених питань, на нашу думку, є побудова національної моделі кібербезпеки інфраструктурних об'єктів та розробка першочергових напрямів діяльності державного та приватного секторів у цій сфері. Україні, що знаходиться у критичному положенні незахищеного кіберпростору, необхідно удосконалити нормативно-правову базу у сфері кібербезпеки, ефективно використовуючи міжнародний досвід і сприяння Заходу у налагоджені ефективної кібербезпекової системи.

Список використаної літератури

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект [Текст] : підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та ін.] ; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К. : ДУТ, 2015. — С. 12.

2. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк // Безпека інформації [Текст]. — 2013. — Т. 19. — № 2. — С. 120.

3. Бурячок В. Л. Інформаційна та кібербезпека… — С. 15.

4. Там само. — С. 12.

5. Черняк О. Р. Тенденції розвитку кіберзагроз у світовому інформаційному просторі / О. Р. Черняк, О. В. Федулов // Сучасні інформаційні технології у сфері безпеки

та оборони [Електронний ресурс]. — 2014. — № 1 (19). — Режим доступу : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?.

6. Дубов Д. В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців [Текст] : аналіт. доп. / Д. В. Дубов, М. А. Ожеван. — К. : НІСД, 2012. — С. 22.

7. Україна та США стали першими у списку жертв кібератак // Канал 24 [Електронний ресурс]. — 2015. — Режим доступу : http://24tv.ua/ukrayina/ukrayina_ta_ssha_stali_pershimi_u_spisku_zhertv_kiberatak/n565572.

8. Костюк І. Україна в фокусі кібератак [Електронний ресурс] / І. Костюк. — Режим доступу : https://scienceukraine.com/sciblogs/ukraina-v-fokusi-kiberatak.

9. Волны российских кибератак напрямую связанны с датами военных событий на востоке Украины // Гордон [Электронный ресурс]. — 2015. — Режим доступа : http://gordonua.com/news/war/Fortune-Volny-rossiyskih-kiberatak-napryamuyu-svyazanny-s-datami-voennyh-sobytiy-na-vostoke-Ukrainy-78512.html.

10. Костюк І. Україна в фокусі кібератак…

11. Крутов М. Кібервійна між Україною і Росією / Марк Крутов // Радіо Свобода [Електронний ресурс]. — 2015. — Режим доступу : http://www.radiosvoboda.org/content/article/25426959.html.

12. Кібервійна проти України: перші жертви і висновки [Електронний ресурс]. — Режим доступу : http://glavcom.ua/publications/334262-kibervijna-proti-ukrajini.-pershi-zhertvi-i-visnovki.html.

13. Там само.

14. Костюк І. Україна в фокусі кібератак…

15. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” [Електронний ресурс] : Указ Президента України № 96/2016 від 15.03.2016 р. — Режим доступу : http://www.president.gov.ua/documents/962016-19836.

Стаття надійшла до редакції 15.06.2016
Схвалена до друку редколегією 04.09.2016

H. Dziana,
N. Dzianyi

NATIONAL CYBER SECURITY POLICY IMPLEMENTATION

The article describes characteristics of implementing national cyber security policy. The cyber attacks on infrastructure objects in Ukraine are analyzed. The problematic issues of ensuring cyber security of infrastructure objects are identified. The ways to improve the national cyber security policy are described in detail.

Key words: information space, information security, cyber space, cyber security, cyber attacks, cyber protection of infrastructure objects.