УДК 354.42/.44:681.142.36

Шеломенцев Володимир Петрович – заступник начальника управління Департаменту МВС України, кандидат юридичних наук, Заслужений юрист України

Основні напрями і суб'єкти забезпечення кібернетичної безпеки України

Стаття присвячена аналізу діяльності щодо забезпечення кібернетичної безпеки України, визначення її основних напрямів і суб'єктів.

Ключові слова: інформаційно-телекомунікаційна система, кіберпростір, кібератака, кіберзагроза, кібербезпека.

Побудова в Україні інформаційного суспільства можлива за умови широкої інтеграції сучасних технологій автоматизованої обробки даних у всі сфери економіки, державного управління та суспільної діяльності. Це різко збільшує залежність реалізації окремих життєво важливих інтересів осіб, суспільства та держави від належного функціонування інформаційно-телекомунікаційних систем (далі – ІТС), за допомогою яких й забезпечується така реалізація.

Значно зростають ризики завдання значної шкоди національним інтересам із використанням впливів кібернетичного характеру, збільшується кількість кібернетичних загроз національній безпеці.

Фахівці вважають, що "кіберзброя та кібератаки за своєю руйнівною потужністю й наслідкам наближаються до зброї масового знищення" [1].

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Тому, розбудова дієвої системи кібернетичної безпеки – одне з найнагальніших завдань забезпечення національної безпеки України.

Різні аспекти забезпечення кібернетичної безпеки досліджували В. М. Бутузов, В. Д. Гавловский, В. О. Голубєв, Д. В. Дубов, Н. А. Ожеван, М. А. Погорецький. Е. В. Рижков, К. В. Тітуніна та інші науковці.

Проте, наукова розробка проблем забезпечення кібернетичної безпеки до сьогодні не носила системного характеру.

Метою статті є аналіз діяльності із забезпечення кібернетичної безпеки України, визначення та деталізація її основних напрямів і суб'єктів.

Під кібернетичною безпекою (кібербезпекою) України розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства в Україні. При цьому, кіберпростір розглядається як специфічне середовище, утворене в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Важливе значення для розбудови системи кібернетичної безпеки України має чітке визначення об'єктів безпеки та основних кіберзагроз. Система кібернетичної безпеки – організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту інтересів у кіберпросторі, що здійснюють узгоджену діяльність у межах законодавства України.

Виходячи зі змісту положень Закону України "Про основи національної безпеки України" [2] та Доктрини інформаційної безпеки України [3], об'єктами кібернетичної безпеки України слід визначити:

– особу – її права і свободи на збирання, зберігання, використання та поширення інформації, що реалізовуються за допомогою ІТС;

– суспільство – та частина його духовних, морально-етичних, культурних, історичних, інтелектуальних і матеріальних цінностей, що формуються з використанням ІТС;

– державу – її суверенітет і недоторканність у кіберпросторі, спроможність виконувати свої функції за допомогою ІТС.

Об'єкти кібернетичної безпеки спрощено можна представити як сукупність суб'єктів відносин, пов'язаних із використанням ІТС, – держава в цілому, державні органи, юридичні (громадські об'єднання, підприємства тощо) та фізичні особи, частина життєво важливих інтересів яких реалізується за допомогою ІТС.

Залежність від належного функціонування ІТС робить суб'єктів таких відносин особливо вразливими для кібернетичного впливу через саму ІТС або її елементи. При цьому, правильно буде говорити саме про безпеку таких суб'єктів, тому що самі ІТС не мають своїх інтересів, яким можна було б завдати шкоди.

Як вбачається із наведеного, основними завданнями системи кібернетичної безпеки слід визначити забезпечення:

– належного (штатного) режиму функціонування ІТС, за допомогою яких реалізуються життєво важливі інтереси особи, суспільства, держави;

– безпечної діяльності у кіберпросторі із задоволення інформаційних потреб користувачів.

Під належним (штатним) режимом функціонування ІТС розуміється функціонування ІТС, яке в повному обсязі відповідає призначен-

ню даної системи та відбувається за стандартним для цієї системи регламентом і технологією виконання. Належне функціонування ІТС передбачає безперервний контроль і керування процесами обробки даних, що гарантує як правильність цих процесів, так і правильність наданих результатів.

У світлі зазначеного, термін "кібернетична безпека" можна розглядати як захищеність належного функціонування ІТС від небажаного для користувачів порушення процесу обробки даних і результатів такої обробки (кіберзагроз).

Під кіберзагрозами розуміються наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Як вбачається, кібернетичний захист ІТС та їх належне функціонування опосередковано забезпечує кібернетичну безпеку особи, суспільства, держави.

Щодо забезпечення безпечної діяльності у кіберпросторі, то суб'єкти відносин, пов'язаних з використанням ІТС, виступають, як правило, учасниками процесів:

– обробки комп'ютерних даних (вироблення та пропонування певного інформаційного продукту, електронної комерції, електронного банкінгу тощо);

– інформаційної взаємодії користувачів кіберпростору (спілкування, пошук і гуртування однодумців, пропаганда власних ідей тощо).

Безпечна діяльність у кіберпросторі передбачає:

– отримання своєчасного доступу (за прийнятний для користувача термін) до необхідних даних;

– дотримання конфіденційності певних даних (наприклад, таких, що становлять таємницю, персональних даних тощо);

– забезпечення вірогідності (повноти, точності, адекватності, цілісності) даних;

– захист від дезінформації, недостовірних і перекручених даних;

– захист певного виду даних від незаконного тиражування;

– встановлення відповідальності за порушення законних прав суб'єктів відносин у кіберпросторі.

Загрози безпечній діяльності у кіберпросторі, пов'язані з протиправним використанням ІТС, і за характером впливу бути поділені на кіберзагрози технічного характеру та загрози психологічного характеру.

Основними загрозами життєво важливим інтересам людини, суспільства, держави, які реалізуються за допомогою інформаційних, телекомунікаційних інформаційно-телекомунікаційних систем, є:

– посягання на Інтернет-ресурси державних органів України з боку спецслужб інших держав, розвідувально-підривна діяльність іноземних спеціальних служб з використанням кіберпростору;

– використання кіберпростору у військових цілях, розробка іноземними державами нових видів зброї кібернетичного характеру;

– можливість втягування України у збройні конфлікти чи у протистояння з іншими державами через використання національного сегменту кіберпростору для здійснення кібератак на об'єкти критичних інформаційних інфраструктур інших держав;

– зростаючі масштаби поширення кіберзлочинності;

– активізація проявів кібертероризму;

– негативні інформаційно-психологічні впливи на суспільну свідомість і маніпулювання нею з кіберпростору;

– несанкціонований доступ і розголошення за допомогою кіберпростору інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації;

– зростання загальної уразливості національного сегменту кіберпростору через значну відмінність у рівнях кіберзахисту державних інформаційних ресурсів, ресурсів комерційних структур, громадських об'єднань та окремих користувачів.

Ураховуючи вищезазначене, основними напрямами забезпечення кібернетичної безпеки України слід визначити:

– кіберзахист об'єктів критичної інформаційної інфраструктури України;

– захист державного суверенітету в кіберпросторі;

– боротьбу з кіберзлочинами та кібертероризмом;

– забезпечення кібернетичної безпеки держави у воєнній сфері та сфері оборони.

В якості об'єктів критичної інформаційної інфраструктури України пропонується розглядати інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, припинення або порушення функціонування яких може призвести до людських жертв, завдання шкоди здоров'ю людей або довкіллю, порушення умов життєдіяльності людей, порушення виробничих або транспортних процесів, значних матеріальних збитків, неспроможності держави виконувати свої функції.

Кібернетична безпека України забезпечується уповноваженими суб'єктами з урахуванням особливостей, визначених Законом України "Про основи національної безпеки України" [2].

Президент України як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандувач Збройних Сил України і Голова Ради національної безпеки

і оборони України здійснює загальне керівництво у сфері кібернетичної безпеки України.

Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади національної політики у сфері кібернетичної безпеки, формує законодавчу базу в цій сфері.

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади забезпечує державний суверенітет і економічну самостійність України у кіберпросторі, розробляє стратегії та програми кібернетичної безпеки України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, безпечного функціонування критичної інформаційної інфраструктури держави.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері кібернетичної безпеки, розробляє пропозиції щодо визначення, коригування засад державної політики у сфері забезпечення кібернетичної безпеки України.

Захист об'єктів критичної інформаційної інфраструктури слід віднести до компетенції Державної служби спеціального зв'язку та захисту інформації, в структурі якої вже функціонують такі підрозділи, як підрозділ реагування на кіберінциденти CERT-UA (скорочена назва від Computer Emergency Response Team of Ukraine) та Центр антивірусного захисту інформації. Було б правильним, якщо б Державна служба спеціального зв'язку та захисту інформації України у межах своїх повноважень відповідно до законів України:

– брала участь у формуванні та реалізації державної політики з питань кіберзахисту об'єктів критичної інформаційної інфраструктури;

– здійснювала координацію органів державної влади, органів місцевого самоврядування з питань захисту об'єктів критичної інформаційної інфраструктури;

– здійснювала державний контроль за ступенем кіберзахисту об'єктів критичної інформаційної інфраструктури;

– здійснювала прогнозування спільно із центральними та місцевими органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями імовірності виникнення кіберінцидентів, визначала показники ризику;

– забезпечувала динамічне визначення наявних і потенційних кіберзагроз об'єктам критичної інформаційної інфраструктури, здійснювала аналіз ризиків, прогнозувала розвиток ситуації та імовірні наслідки реалізації таких загроз;

– здійснювала методичне керівництво щодо забезпечення належного функціонування об'єктів критичної інформаційної інфраструктури;

– затверджувала загальнодержавні правила захисту об'єктів критичної інформаційної інфраструктури, а також вимоги, інструкції і методики, інші нормативно-правові акти у цій сфері, які є обов'язковими для всіх підприємств, установ, організацій;

– виступала замовником наукових робіт, брала участь у проведенні прикладних науково-дослідних робіт щодо захисту об'єктів критичної інформаційної інфраструктури, розробляла та затверджувала галузеві стандарти з питань кібернетичної безпеки;

– своєчасно сповіщала власників об'єктів критичної інформаційної інфраструктури про існуючі кіберзагрози, забезпечувала обмін інформацією про кіберінциденти;

– брала участь у роботі комісій з розслідування кіберінцидентів на об'єктах критичної інформаційної інфраструктури, вживала заходів щодо усунення їх причин;

– проводила експертизи кіберінцидентів і визначала їх рівні;

– проводила професійну підготовку, підвищення кваліфікації та перепідготовку фахівців з питань захисту об'єктів критичної інформаційної інфраструктури;

– створила та вела Державний реєстр об'єктів критичної інформаційної інфраструктури.

Розвідувальні органи України в межах своїх повноважень здійснюють спеціальні заходи впливу, спрямовані на підтримку національних інтересів і державної політики України у кіберпросторі, забезпечують добування, аналітичну обробку та надання в установленому порядку інформації про кіберзагрози, пов'язані з діяльністю іноземних і міжнародних злочинних організацій за межами України.

Правоохоронні органи ведуть боротьбу з кіберзлочинами і протидіють кібертероризму, забезпечують безпеку користування ресурсами національного сегменту кіберпростору.

Боротьбу з кіберзлочинністю та кібертероризмом у межах своїх повноважень відповідно до законів України здійснюють Міністерство внутрішніх справ України та Служба безпеки України. Наприклад, Міністерство внутрішніх справ України:

– бере участь у формуванні та реалізації державної політики з питань боротьби з кіберзлочинами, у т. ч. такими, що вчиняються з терористичною метою;

– вживає необхідних заходів щодо попередження, своєчасного виявлення, припинення і розкриття кіберзлочинів;

– забезпечує належне функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні кіберзлочинів;

– забезпечує взаємодію з операторами та провайдерами телекомунікацій з питань попередження кіберінцидентів кримінального характеру;

– взаємодіє з компетентними органами інших країн у межах надання міжнародно-правової допомоги з протидії кіберзлочинам.

Воєнна організація держави забезпечує оборону України, захист її суверенітету в кіберпросторі, вживає заходів з протидії і нейтралізації кібернетичних загроз національним інтересам України у воєнній сфері та сфері оборони.

Міністерство оборони України у межах своїх повноважень відповідно до законів України забезпечує кібернетичну безпеку держави у воєнній сфері та сфері оборони шляхом:

– участі у формуванні та реалізації державної політики з питань кібернетичної безпеки у воєнній сфері та сфері оборони;

– прогнозування та оцінки кіберзагроз воєнного характеру;

– підтримання належного рівня боєздатності Збройних Сил України у кіберпросторі;

– протидії воєнним загрозам національному сегменту кіберпростору;

– розвитку та кіберзахисту власної інформаційної інфраструктури та ресурсів;

– участі у підготовці об'єктів критичної інформаційної інфраструктури до функціонування в особливий період і в умовах воєнного стану.

Інші міністерства та центральні органи виконавчої влади України в межах своїх повноважень забезпечують виконання передбачених Конституцією і законами України, актами Президента України, Кабінету Міністрів України завдань, здійснюють реалізацію програм у сфері кібернетичної безпеки, підтримують у стані готовності до застосування сили та засоби забезпечення кібернетичної безпеки.

Місцеві державні адміністрації та органи місцевого самоврядування забезпечують вирішення питань у сфері кібернетичної безпеки, віднесених законодавством до їхньої компетенції.

Громадяни України добровільно і в порядку виконання конституційних обов'язків здійснюють заходи, визначені законодавством України щодо забезпечення кібернетичної безпеки; як безпосередньо, так і через об'єднання громадян привертають увагу суспільних і державних інститутів до небезпечних явищ і процесів у національному сегменті кіберпростору.

Побудова дієвої системи кібернетичної безпеки України вимагає чіткого визначення державної політики у цій сфері та випереджального правового реагування на динамічні зміни, що відбуваються у кіберпросторі.

Список використаних джерел

1. Брито Д. Кибератаки: угроза преувеличена для контроля Интернета [Электронный ресурс] / Джерри Брито, Тэйт Уоткинс. – 2009. – Режим доступу : http://papinaziat. ru/? tag=кибербезопасности.

2. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

3. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіц. вісн. України. – 2009. – № 52. – Ст. 1783. – С. 7. – 20 лип.

Статья посвящена анализу деятельности по обеспечению кибернетической безопасности Украины, определению ее основных направлений и субъектов.

The article deals with the analysis of the activities to ensure the cyber security of Ukraine, the definition of its main directions and subjects.

Стаття надійшла до редакції журналу 29 березня 2013 року.