УДК 343.9

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

Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення

Стаття присвячена аналізу стану правового забезпечення системи кібернетичної безпеки України.

Ключові слова: комп'ютерна система, кіберпростір, кібератака, кіберзагроза, кібербезпека.

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. 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 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 такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 році доручалося розробити Кабінету Міністрів України за участю Служби безпеки України [1].

Водночас, недосконалість національного законодавства у сфері забезпечення кібернетичної безпеки значно підвищує ймовірність реалізації таких загроз, що негативно впливає на загальний рівень національної безпеки України.

Різні аспекти правового забезпечення протидії кіберзагрозам досліджували В. М. Бутузов, В. Д. Гавловский, В. О. Голубєв, Д. В. Дубов, В. А. Номоконов, Н. А. Ожеван, М. А. Погорецький. Е. В. Рижков, К. В. Тітуніна, Т. Л. Тропіна та інші науковці.

Проте, наукова розробка проблем правового забезпечення системи кібернетичної безпеки до теперішнього часу не носила системного характеру, розглядалися в основному питання, пов'язані з протидією правової кіберзлочинності та кібертероризму.

Метою статті є висвітлення основних проблем правового забезпечення системи кібернетичної безпеки України та визначення напрямів їх вирішення.

Правову основу кібернетичної безпеки України становлять Конституція України, закони України "Про основи національної безпеки", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти.

Водночас, аналіз чинного законодавства дозволяє визначити як основну проблему правового забезпечення системи кібернетичної безпеки України відсутність розробленого та нормативно закріпленого понятійного апарата у сфері кібернетичної безпеки.

Недоліки понятійного апарата у сфері забезпечення кібернетичної безпеки не дозволяють: визначити ознаки та об'єктивно оцінити основні загрози у національному сегменті кіберпростору; визначити найбільш ефективні заходи забезпечення кібернетичної безпеки; чітко сформулювати завдання та функції суб'єктів кібернетичної безпеки тощо. У законодавстві відсутнє визначення не тільки поняття "кібернетична безпека (кібербезпека)", але й таких понять як "кібернетичний простір (кіберпростір)", "кібернетична загроза (кіберзагроза)", "кібернетична атака (кібератака)", "кібернетичний захист (кіберзахист)", "кібернетичний злочин (кіберзлочин)", "кіберзлочинність" тощо.

При визначенні термінів пропонується надавати їх у більш широкому розумінні, враховуючи вже наявні напрацювання у таких галузях науки як кібернетика, інформатика, безпекознавство, кримінальне право тощо.

Під кібернетичною безпекою розуміють стан захищеності життєво важливих прав та інтересів людини, суспільства, держави у кіберпросторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань [2, с. 176]. Проте, враховуючи інші наукові підходи до визначення безпеки, кібернетичну безпеку пропонується розуміти як стан захищеності життєво важливих інтересів особи, суспільства, держави від зовнішніх і внутрішніх загроз, пов'язаних з використанням ресурсів інформаційно-телекомунікаційних систем (іншими словами ресурсами кіберпростору).

Також, кібернетичну безпеку пропонується розглядати як складову інформаційної безпеки – стану захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [3]. В свою чергу, інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки [4], а також важливою самостійною сферою забезпечення національної безпеки [5].

Як вбачається, кібернетична безпека охоплює лише ту частину інформаційної сфери, в якій для обробки інформації застосовуються інформаційно-телекомунікаційні системи.

Кібернетична безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм.

Стратегія кібернетичної безпеки України повинна бути розроблена у розвиток Доктрини інформаційної безпеки України. Вона має визначати мету і головні пріоритети діяльності держави у цій сфері, а також коротко-, середньо- і довгострокові цілі, методи їх досягнення; стратегічні завдання та засоби зменшення уразливості об'єктів критичної інфраструктури у національному кібернетичному просторі; основні напрями, підходи та методи забезпечення кібернетичної безпеки України. Саме у Стратегії кібернетичної безпеки України доцільно передбачити основні напрями державної політики з питань кібернетичної безпеки України, а саме: забезпечення суверенітету України у кіберпросторі, наповнення кіберпростору достовірною інформацією про Україну; створення сприятливих зовнішньополітичних умов для прогресивного розвитку національного сегменту кіберпростору; запобігання втручанню у внутрішні справи України і відвернення посягань на її Інтернет-ресурси з боку інших держав; забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібернетичної безпеки; участь України в міжнародному співробітництві у сфері боротьби з кіберзлочинністю та кібертероризмом; зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби у кіберпросторі з проявами організованої злочинності та кібертероризму; боротьба з організованими злочинними угрупованнями, в тому числі міжнародними, які намагаються діяти у національному сегменті кіберпростору; забезпечення максимальної ефективності Збройних Сил України у кіберпросторі та їх здатності давати адекватну відповідь реальним і по-

тенційним кібернетичним загрозам Україні; запобігання проявам екстремізму в національному сегменті кіберпростору; посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій; забезпечення необхідних умов для реалізації прав інтелектуальної власності у національному сегменті кіберпростору; створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів.

Ідеї Стратегії кібернетичної безпеки України повинні отримати розвиток у положеннях базового закону в цій сфері, а також змінах і доповненнях до інших законів України, що регулюють відносини у сфері кібернетичної безпеки.

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 регулюватися 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).

Саме кіберзлочини (несанкціоноване втручання в роботу комп'ютерних систем; створення шкідливих програмних чи технічних засобів; несанкціоновані дії з інформацією, яка оброблюється в комп'ютерних системах; перешкоджання роботі комп'ютерних систем) є тими засобами, за допомогою яких здійснюються кібернетичні атаки різного характеру на об'єкти критичної інфраструктури держави.

Виходячи із зазначеного, при конструюванні норм і структури законопроекту "Про основи кібернетичної безпеки України" логічно було б виходити із положень Доктрини інформаційної безпеки України та Закону України "Про основи національної безпеки".

Необхідно вказати, що в Доктрині інформаційної безпеки України [5] визначено: основні засади інформаційної безпеки України (принципи забезпечення інформаційної безпеки України); місце інформаційної безпеки в системі забезпечення національної безпеки України (сформульовано: життєво важливі інтереси в інформаційній сфері для особи, суспільства, держави; реальні та потенційні загрози інформаційній безпеці України на сучасному етапі у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері, внутрішньополітичній сфері, економічній сфері; соціальній та гуманітарній сферах; науково-технологічній сфері, екологічній сфері).

Серед основних принципів забезпечення кібернетичної безпеки варто визначити такі, як: своєчасність і адекватність заходів кібернетичного захисту життєво важливих інтересів людини і громадянина, суспільства і держави реальним і потенційним кіберзагрозам; чітке роз-

межування повноважень і взаємодію органів державної влади у забезпеченні кібернетичної безпеки; використання в інтересах України міжнародних механізмів забезпечення кібернетичної безпеки.

При цьому, систему кібернетичної безпеки пропонується визначити у законопроекті "Про основи кібернетичної безпеки України" як сукупність спеціальних суб'єктів забезпечення кібербезпеки, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних і технічних заходів.

Аналіз розбудови систем кібербезпеки у провідних державах світу свідчить, що основними тенденціями у цій сфері є відповідна системна реорганізація сектору безпеки та створення спеціалізованих підрозділів із захисту національних інтересів у кіберпросторі.

Важливим є питання визначення державного органу (відповідальної особи), який би забезпечував координацію з питань кібербезпеки. Таким органом може бути Міжвідомча комісія з питань забезпечення кібернетичної безпеки при РНБО України, на яку покласти функції координації розробки і виконання заходів щодо забезпечення кібернетичної безпеки України.

До загальних суб'єктів забезпечення кібернетичної безпеки України доцільно віднести: центральний орган виконавчої влади, що реалізує державну політику в сфері захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації; центральний орган виконавчої влади, що реалізує державну політику в сфері інформатизації та телекомунікацій; підрозділи розвідувальних органів України, що виконують завдання із забезпечення кібернетичної безпеки України; органи державної влади, а також підприємства, установи, організації, у власності яких перебувають об'єкти, віднесені до критичної інфраструктури; правоохоронні органи, що здійснюють досудове слідство в справах про кіберзлочини; Збройні Сили України, що реагують на військову агресію, у т. ч. із застосуванням кібернетичної зброї; підприємства, установи, організації, що проводять господарську діяльність у кіберпросторі, в т. ч. пов'язану із захистом інформаційних ресурсів.

Водночас, з числа загальних суб'єктів необхідно окремо виділити спеціальних суб'єктів забезпечення кібернетичної безпеки, якими є суб'єкти протидії кіберзлочинності та кібертероризму (Міністерство внутрішніх справ України; Служба безпеки України; Міністерство юстиції України; Генеральна прокуратура України) та суб'єкти забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури (Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; власники об'єктів національної критичної інфраструктури).

Виходячи з положень Доктрини інформаційної безпеки України, об'єктами кібернетичної безпеки (як складової національної безпеки) слід визначити:

– людину і громадянина – їхні права і свободи, що реалізовуються за допомогою інформаційно-телекомунікаційних систем;

– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності у сфері використання інформаційно-телекомунікаційних систем;

– державу – її суверенітет і недоторканність у кібернетичному просторі об'єктів національної критичної інфраструктури.

Крім того, у законопроекті доцільно також: надати перелік основних видів кібернетичних загроз для людини і громадянина, суспільства та держави, у тому числі й для об'єктів національної критичної інфраструктури; визначити перелік основних ознак об'єктів національної критичної інфраструктури, що потребують захисту від кібератак.

Кібернетичні загрози являють собою загрози, реалізація яких пов'язана з використанням відповідних ресурсів інформаційно-телекомунікаційних систем. Уразливими для реалізації кібернетичних загроз є об'єкти, функціонування комп'ютерних систем яких пов'язане з використанням ресурсів кіберпростору. Тобто об'єкти, завдання шкоди яким можливе шляхом деструктивного кібернетичного впливу (кібернетичної атаки) – інформаційного впливу з використанням кіберресурсів, спрямованого на уразливості комп'ютерних систем таких об'єктів.

Крім того, слід зауважити, що відповідно до Закону України "Про Концепцію Національної програми інформатизації" [4], такі системи варто розглядати як окремі складові національної інформаційної інфраструктури або Національної інфраструктури інформатизації.

Тому, правильніше буде розглядати об'єктами кібербезпеки у базовому законопроекті або інформаційно-телекомунікаційні системи об'єктів національної критичної інфраструктури, або об'єкти національної інформаційної критичної інфраструктури.

До об'єктів національної критичної інфраструктури, що потребують захисту від кібератак, необхідно віднести об'єкти, реалізація кібернетичних загроз щодо яких може призвести до настання таких наслідків як: надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки; блокування роботи державних органів; блокування діяльності органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці; масові заворушення.

Як вбачається, не всі об'єкти такої інфраструктури є уразливими для кібернетичних впливів (тобто діяльність не всіх об'єктів критично залежить від нормального функціонування певних комп'ютерних систем). Водночас, кожній комп'ютерній системі, що використовується на окремому об'єкті критичної національної інфраструктури, властиві конкретні уразливості, а значить і відповідні загрози.

Тобто, лише визначивши об'єкти критичної національної інфраструктури та встановивши основні зовнішні та внутрішні загрози кібернетичного характеру, можна приступити до формування системи безпеки, ефективність якої буде обумовлена підбором: найбільш ефективних заходів захисту від різних видів кібернетичних загроз; суб'єктів, здатних забезпечити вжиття відповідних заходів захисту.

Перелік об'єктів національної критичної інфраструктури та їх категорії повинен встановлюватися Кабінетом Міністрів України. Об'єктам національної критичної інфраструктури залежно від ступенів важливості, вразливості, захисту, прогнозованих наслідків, що можуть настати в результаті реалізації кібернетичної загрози щодо систем і мереж, які в ньому функціонують, наявної в них інформації, та програмного забезпечення, призначеного для її обробки, присвоюються відповідні категорії важливості.

Вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України обумовлюється 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 та 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 – 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 й технічних заходів.

З метою приведення національного законодавства у відповідність до положень Конвенції про кіберзлочинність щодо процедурних питань протидії кіберзлочинам необхідно внести відповідні зміни та доповнення до законів України "Про міліцію", "Про Службу безпеку України", "Про оперативно-розшукову діяльність", "Про організаційно-правові основи боротьби з організованою злочинністю" та ін.

Таким чином, до основних напрямів формування правової основи забезпечення кібербезпеки України слід віднести:

– нормативне закріплення понятійного апарата у сфері кібернетичної безпеки – створення, за участю зацікавлених відомств, базового документу (тезаурусу, ДСТУ) із визначенням основних понять у сфері кібербезпеки та забезпечення імплементації необхідних термінів до чинного законодавства України, а саме шляхом внесення змін і доповнень до законів України "Про інформацію", "Про захист інформації в інформаційно-телекомуніаційних системах", "Про основи національної безпеки України", "Про телекомунікації" тощо;

– розроблення Стратегії кібернетичної безпеки України та подання її на затвердження Президентові України;

– розроблення та подання на розгляд Верховної Ради України проекту Закону України "Про основи кібернетичної безпеки України", в якому, зокрема: а) визначити понятійний апарат, перелік основних загроз кібернетичній безпеці України; б) передбачити створення правової основи та матеріально-технічної бази системи кібернетичної безпеки України; в) визначити критерії віднесення об'єктів національного сегменту кіберпростору всіх форм власності до критичної інфраструктури, порядок формування переліку таких об'єктів; г) визначити компетенцію державних структур у сфері кібербезпеки та їх форми взаємодії між собою і приватним сектором.

– внесення, з метою приведення національного законодавства у відповідність до положень Конвенції Ради Європи про кіберзлочинність [6], відповідних змін і доповнень до законів України "Про міліцію", "Про Службу безпеку України", "Про оперативно-розшукову діяльність", "Про організаційно-правові основи боротьби з організованою злочинністю" та ін.

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 з 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.

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. Про рішення Ради національної безпеки і оборони України від 17 листопада 2010 року "Про виклики та загрози національній безпеці України у 2011 році" : Указ Президента України від 10 груд. 2010 р. № 1119/2010 / [Електронний ресурс]. – Режим доступу :

http://www. president. gov. ua/documents/12624. html.

2. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січ. 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

4. Про Концепцію Національної програми інформатизації : Закон України від 4 лют. 1998 р. // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 182.

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

6. Про кіберзлочинність : Конвенція Ради Європи // Офіц. вісник України. – 2007. – № 65. – Ст. 2535. – С. 107. – Код акту 40846/2007. – 10 верес.

Статья посвящена анализу правового обеспечения системы кибернетической безопасности Украины.

The article is devoted to the analysis of the legal providing of cybersecurity system of Ukraine.

Стаття надійшла до редакції журналу 1 червня 2012 року.