УДК 343.9

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

Місце та роль МВС України у національній системі кібернетичної безпеки

У статті розглядаються питання розбудови національної системи кібернетичної безпеки, розкривається місце та роль МВС України у такій системі, визначаються основні функції МВС України у підсистемі протидії кіберзлочинності.

Ключові слова: кібернетична безпека, система кібербезпеки, суб'єкти забезпечення кібербезпеки, кіберзлочинність, протидія кіберзлочинності.

Постановка проблеми. Залежність об'єктів критичної інфраструктури України від широкого використання інформаційно-телекомунікаційних систем робить їх уразливими для протиправного впливу з використанням ресурсів кібернетичного простору та підвищує ризик виникнення надзвичайних ситуацій, створює реальні загрози життєдіяльності людини, суспільства, держави, подальшому соціально-економічному розвитку та національній безпеці України.

Кібернетичний простір осмислюється як нове середовище прояву життєво важливих інтересів особи, суспільства, держави, які реалізуються за допомогою інформаційно-телекомунікаційних систем і також потребують захисту.

Питання реалізації життєво важливих інтересів особи, суспільства, держави у кібернетичному просторі тісно пов'язані із забезпеченням їх кібернетичної безпеки (кібербезпеки), під якою розуміють стан захищеності важливих інтересів особи, суспільства, держави від зовнішніх і внутрішніх загроз, пов'язаних з використанням деструктивного кібернетичного впливу на інформаційно-телекомунікаційні системи (кіберзагроз), що забезпечують реалізацію таких інтересів.

Необхідність ефективної протидії основним кіберзагрозам потребує осмислення місця та ролі Міністерства внутрішніх справ України (далі – МВС України) у системі кібернетичної безпеки України.

Стан дослідження. Окремі аспекти визначення ролі та місця МВС України у національній системі кібернетичної безпеки розглядали В. М. Бутузов, В. Д. Гавловський, М. А. Погорецький, К. В. Титуніна та інші науковці.

Проте, аналіз наукових джерел свідчить, що дослідниками розглянуто лише загальні питання розбудови національної системи кібернетичної безпеки. Водночас, розкриття сутності функцій та повноважень МВС України у такій системі дозволить підвищити ефективність діяльності як органів внутрішніх справ у цілому, так і спеціалізованих підрозділів з протидії кібернетичній злочинності.

Метою статті є розкриття місця та ролі МВС України у національній системі кібернетичної безпеки, основних функцій МВС України у підсистемі протидії кіберзлочинності.

Виклад основного матеріалу. Сьогодні на розгляді у Верховній Раді України знаходяться два законопроекти з кібербезпеки:

– Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України (реєстр. № 2483 від 7 березня 2013 року), поданий Кабінетом Міністрів України [1];

– Про кібернетичну безпеку України (реєстр. № 2207а від 4 червня 2013 року), який подали народні депутати України В. М. Олійник, Ю. П. Самойленко, О. І. Кузьмук [2].

Необхідність прийняття законопроекту про кібернетичну безпеку України обумовлена неврегульованістю на законодавчому рівні відносин, пов'язаних із забезпеченням національних інтересів у кіберпросторі. Такий законопроект повинен стати основою для розроблення єдиної державної політики з питань забезпечення кібернетичної безпеки України.

Відповідно до законопроекту, поданого Кабінетом Міністрів України, до Закону України "Про основи національної безпеки України" пропонується внести зміни в частині визначення основних реальних і потенційних загроз національній безпеці України кібернетичного характеру, основних напрямів державної політики та основних функції суб'єктів забезпечення національної безпеки в цій сфері, а також уведення таких основоположних понять, як "кібернетична безпека (кібербезпека)" та "кібернетичний простір (кіберпростір)". У такий спосіб автори законопроекту намагаються закласти необхідну правову основу для подальшої нормотворчої діяльності (як на законодавчому, так і на підзаконному рівні) з питань забезпечення кібербезпеки.

У законопроекті, поданому народними депутатами України, визначаються об'єкти, суб'єкти забезпечення кібернетичної безпеки, ос-

новні функції та повноваження цих суб'єктів. Тобто, вбачаються контури певної системи кібернетичної безпеки, в якості об'єктів якої визначено людину суспільство, державу.

Під системою кібернетичної безпеки України розуміється сукупність суб'єктів забезпечення кібернетичної безпеки України, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних й технічних заходів.

Кіберзагрози виявляються в усіх сферах національної безпеки, а не лише в інформаційній. Тобто, кібербезпеку доцільно сприймати не як окрему складову національної безпеки, а як прояв національної безпеки у новому середовищі (кіберпросторі) та у новому вигляді (програмно-математичному).

Систему кібернетичної безпеки слід розглядати як похідну від системи забезпечення національної безпеки України (у кібернетичному середовищі). У такому середовищі присутні всі сфери забезпечення національної безпеки (воєнна, політична, економічна, фінансова, інформаційна тощо), а значить повинні реалізовуватись й усі основні функції суб'єктів забезпечення національної безпеки.

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. Реалізація конкретних функцій суб'єктами забезпечення кібернетичної безпеки України обумовлюється їх компетенцією та можливістю своєчасного вжиття заходів, адекватних характеру і масштабам реальних і потенційних кіберзагроз життєво важливим інтересам особи, суспільства й держави.

Метою функціонування національної системи кібернетичної безпеки слід визначити забезпечення безпеки держави у кібернетичному просторі шляхом забезпечення захисту об'єктів критичної інформаційної інфраструктури, запобігання, виявлення та припинення злочинів і правопорушень у кібернетичному просторі, здійснення розвідувальних та оборонних операцій, забезпечення злагодженого функціонування суб'єктів забезпечення кібернетичної безпеки держави.

Відповідно до основних завдань кібербезпеки, у системі кібернетичної безпеки, доцільно виділити такі функціональні підсистеми:

– протидії кіберзлочинності;

– кіберзахисту об'єктів критичної інформаційної інфраструктури;

– реагування на кіберзагрози державному суверенітету в кіберпросторі;

– забезпечення кібербезпеки у воєнній сфері та сфері оборони.

При цьому, як вбачається, відповідно до Конвенції Ради Європи про кіберзлочинність і Доктрини інформаційної безпеки України, кібе-

рзлочинність слід розглядати як основну загрозу національній безпеці у кіберпросторі – саме кіберзлочини є тим засобом, за допомогою якого у кіберпросторі можуть здійснюватись диверсії, терористичні акти, акти війни тощо.

До числа основних причин поширення кіберзлочинності відносять нездатність більшості держав здійснювати ефективний контроль над національним сегментом інформаційного простору через те, що: значна частина світової спільноти вважає це порушенням прав і свобод; розвиток правової бази відстає від розвитку інформаційних технологій (чинне законодавство не встигає за процесом інформатизації, впровадженням усе новіших технологій обробки інформації); відсутні відповідні спеціалізовані підрозділи правоохоронних органів; упровадження такого контролю потребує значних фінансових, технологічних і кадрових ресурсів тощо.

Дослідниками відмічається, що висока соціальна небезпека кіберзлочинності випливає, насамперед, із суспільних відносин, яким вона загрожує, її транснаціонального та організованого характеру, високого рівня латентності. Крім того, кіберзлочинність стала одним із найбільш прибуткових видів діяльності організованих злочинних угруповань.

У 2001 році було прийнято нову редакцію Кримінального кодексу України, в якій вперше було виділено окремий вид злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (розділ XVI КК України) [3]. Аналіз об'єктивної сторони злочинів даного виду вказує на те, що вона відбувається в окремому середовищі комп'ютеризованої обробки інформації. Вказівка на використання комп'ютерних систем і мереж дозволяє розглядати такі злочини як вчинені у кіберпросторі.

У 2005 році Україною було ратифіковано Конвенцію Ради Європи про кіберзлочинність [4], якою запропоновано перелік кіберзлочинів. Аналіз положень даної Конвенції дозволяє розглядати кіберзлочини як злочини у середовищі комп'ютерних систем, вчинені з використанням цих комп'ютерних систем або їх елементів.

Протидія кіберзлочинності розглядається авторами законопроекту 2207а як одне з основних завдань кібернетичної безпеки. До інших завдань вони відносять:

– розроблення та впровадження дієвих механізмів захисту конституційних прав і свобод особи на збирання, зберігання, використання та поширення інформації у кіберпросторі;

– запобігання актам застосування збройної сили проти України з використанням кіберпростору;

– забезпечення державної безпеки у кіберпросторі;

– систематичне спостереження за проявами кібертероризму;

– захист об'єктів критичної інформаційної інфраструктури держави [2].

Розбудова системи кібербезпеки в Україні (в аспекті протидії кіберзлочинності) вимагає вирішення таких питань організаційного характеру, як:

– чітке визначення функцій суб'єктів протидії кіберзлочинності та розподілу повноважень між ними;

– забезпечення належної координації діяльності як суб'єктів забезпечення кібербезпеки загалом, так і суб'єктів протидії кіберзлочинності;

– розробка та впровадження нових підходів, форм і методів протидії кіберзлочинності, відмінних від традиційних;

– запровадження дієвих стимулів для залучення до спеціалізованих підрозділів по боротьбі з кіберзлочинністю фахівців відповідного рівня кваліфікації.

Мабуть, ураховуючи зазначене, автори законопроекту 2207а пропонують визначити МВС України одним із основних суб'єктів забезпечення кібернетичної безпеки України, який:

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

– забезпечує у межах своєї компетенції безпеку громадян у національному сегменті кіберпростору;

– 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 рамках надання міжнародно-правової допомоги у протидії кіберзлочинам [2].

Тобто, МВС України пропонується розглядати в якості головного суб'єкта функціональної підсистеми протидії кіберзлочинності – складової національної системи кібернетичної безпеки України. Уточнення ролі та місця МВС України у системі кібернетичної безпеки дозволить значно підвищити ефективність протидії кіберзлочинності.

Функціональні підсистеми системи кібернетичної безпеки повинні утворюватись центральними органами виконавчої влади у відповідній сфері управління. Перелік центральних органів виконавчої влади, що створюють функціональні підсистеми, повинні визначатися Положенням про національну систему кібернетичної безпеки.

Слід відмітити, що у 2010 році Кабінету Міністрів України за участю Служби безпеки України вже доручалось розробити та подати на розгляд РНБО України пропозиції щодо створення загальнодержавної системи протидії кіберзлочинності [5].

Відсутність в Україні дієвої системи кібернетичної безпеки поряд із зростанням кількості реальних кіберзагроз негативно впливає на загальний рівень національної безпеки України. Сьогодні МВС України можна розглядати скоріше як суб'єкт підсистеми протидії кіберзлочинності, а ніж суб'єкт забезпечення кібернетичної безпеки України.

Так, відповідно до статті 216 КПК України [6] досудове розслідування кримінальних правопорушень, передбачених розділом XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" КК України [3], здійснюють слідчі органів внутрішніх справ.

Також, відповідно до Закону України "Про ратифікацію Конвенції про кіберзлочинність" [7], на Міністерство внутрішніх справ України покладено повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних із комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються в учиненні таких злочинів, а також збирання доказів у електронній формі.

Загальні вимоги до розбудови системи кібернетичної безпеки в Україні повинні враховувати світову тенденцію до зміщення основних акцентів забезпечення кібербезпеки з правоохоронних аспектів (протидія проникненню криміналу до кіберпростору, боротьба з кіберзлочинністю) до воєнних і розвідувальних, а також протидії кібертероризму.

У процесі створення ефективної національної системи кібернетичної безпеки, акцент ставиться на формуванні відносин та об'єднанні зусиль різних силових відомств України. Водночас, ефективність боротьби з кіберзлочинами залежить від належного рівня співробітництва між МВС України та компетентними органами інших країн. З урахуванням міжнародного досвіду для підвищення рівня міжнародного співробітництва у сфері протидії кіберзлочинності необхідно:

1. Активізувати роботу в форматі комісій, експертних груп, інших дорадчих і координуючих органів ООН з питань протидії кіберзлочинності.

2. Здійснювати формування підсистеми протидії кіберзлочинності з урахуванням тенденцій глобальної кібербезпеки.

3. Забезпечити подальший розвиток міжнародного співробітництва з якомога ширшим колом компетентних органів інших країн – як на двохсторонній, так і багатосторонній основі – передусім з питань щодо:

– своєчасного виявлення, аналізу та нейтралізації кібернетичних атак кримінального характеру, а також їх попередження;

– оперативного обміну інформацією про кібернетичні інциденти кримінального характеру;

– обміну методиками боротьби з окремими видами кіберзлочинів;

– проведення спільних заходів у кіберпросторі з протидії кіберзлочинності.

4. Налагодити дієву співпрацю з Центром передового досвіду з кіберзахисту (м. Таллінн, Естонська Республіка) з метою обміну досвідом і проведення спільних заходів.

5. Розробити пропозиції з удосконалення національного законодавства щодо спрощення процедур міжнародного співробітництва при реагуванні на кібернетичні інциденти кримінального характеру, забезпечити імплементацію необхідної термінології у сфері кібербезпеки до чинного законодавства України.

6. Сприяти проведенню міжнародних заходів і навчань з питань протидії кіберзлочинності.

Висновок. Підсистему протидії кіберзлочинності слід розглядати як сукупність спеціальних суб'єктів забезпечення протидії кіберзлочинності, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних і технічних заходів. Положення про національну систему кібернетичної безпеки та положення про функціональні підсистеми повинні затверджуватися Кабінетом Міністрів України.

До основних функцій МВС України, як суб'єкта протидії кібернетичній злочинності, слід віднести:

– вироблення та періодичне уточнення стратегій і програм у сфері протидії кібернетичній злочинності, планування й здійснення конкретних заходів щодо протидії кібернетичній злочинності;

– удосконалення нормативно-правової бази у сфері протидії кібернетичній злочинності;

– створення і підтримання в постійній готовності систем моніторингу аномальних процесів у кіберпросторі з метою кібернетичних злочинів;

– розроблення науково обґрунтованих пропозицій і рекомендацій щодо протидії кібернетичній злочинності;

– підготовку сил і засобів реагування на кібернетичні атаки кримінального характеру;

– запобігання кіберінцидентам та усунення причин їх виникнення;

– проведення професійної підготовки, підвищення кваліфікації та перепідготовки фахівців з питань протидії кібернетичній злочинності;

– проведення спільних планових та оперативних заходів у рамках міжнародних організацій і договорів у сфері протидії кібернетичній злочинності.

При цьому, як свідчить досвід протидії кіберзлочинності, відповідна система, залежно від особливостей і масштабів наслідків кібератак на об'єкти критичної інформаційної інфраструктури, повинна функціонувати у режимах: повсякденного функціонування; підвищеної готовності; надзвичайної ситуації.

Список використаних джерел

1. Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України : законопроект від 7 берез. 2013 р. реєстр. № 2483 / [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998.

2. Про кібернетичну безпеку України : законопроект від 4 черв. 2013 р. реєстр. № 2207а / [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47240.

3. Кримінальний кодекс України // Відомості Верховної Ради України. – 2001. – № № 25–26. – Ст. 131.

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

5. 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.

6. Кримінально-процесуальний кодекс України. Науково-практичний коментар : [у 2 т.] / О. М. Бандурка, Є.М. Блажівський, Є. П. Бурдоль та ін. ; [за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова]. – Х. : Право, 2012. – Т. 1. – 776 с.

7. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.

В статье рассматриваются вопросы построения национальной системы кибернетической безопасности, раскрывается место и роль МВД Украины в такой системе, определяются основные функции МВД Украины в подсистеме противодействия киберпреступности.

The article deals with the questions of construction of the national system of cybernetic security, the place and the role of the MIA of Ukraine in such system are examined, the basic functions of the MIA of Ukraine in the subsystem of counteraction cybercrime are determined.

Стаття надійшла до редакції журналу 27 листопада 2013 року.