УДК 351.746:007

ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук, старший науковий співробітник,*
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України

ЗАХИСТ ІНФОРМАЦІЇ ШЛЯХОМ ПОСИЛЕННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ КІБЕРАТАКАМ

Анотація. *У статті розглянуто окремі аспекти захисту інформації шляхом посилення ефективності протидії кібератакам. Проаналізовано стан виконання рішення РНБО України щодо розмежування підслідності розслідування кіберзлочинів.*

Ключові слова: *захист інформації, протидія кібератакам, посилення відповідальності, розмежування підслідності.*

Summary. *The article deals with some aspects of information security by enhancing the effectiveness of counteracting cyber attacks. The State of Implementation of the NSDC Decision on Delimitation of the Continuity of Investigation of Cybercrimes is analyzed.*

Keywords: *protection of information, counteraction to cyber attacks, strengthening of responsibility, delimitation of jurisdiction.*

Аннотация. *В статье рассмотрены отдельные аспекты защиты информации путём усиления эффективности противодействия кибератакам. Проанализировано состояние выполнения решения СНБО Украины относительно разграничения подследственности расследования киберпреступлений.*

Ключевые слова: *защита информации, противодействие кибератакам, усиление ответственности, разграничения подследственности.*

Постановка проблеми. Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1].

Кібератаки дедалі частіше стають інструментом швидкого досягнення необхідних результатів як в економічній, так і політичній сферах. Серед іншого, кібератаки здійснюються з метою викрадання конфіденційної інформації, персональних даних або їх знищення, блокування роботи інфраструктури тощо.

При цьому визначити ініціаторів атак, незалежно від того, чи це урядові структури або приватні групи зловмисників, які заробляють таким чином гроші, – стає також дедалі важче.

Служба безпеки України протягом останніх місяців реєструє зростаючу кількість розповсюджуваних атак на кшталт “відмова в обслуговуванні” і шахрайських спроб отримати доступ до інформації, що знаходиться на комп’ютерах міністерств та інших державних структур.

Основними об’єктами протиправних спрямувань залишаються інформаційно-комунікаційні системи органів державної влади, державні реєстри та бази даних, а також автоматизовані системи управління технологічними процесами об’єктів критичної інфраструктури енергетичного, транспортного та фінансового секторів.

Отже, питання захисту критичної інформаційної інфраструктури та захисту інформації зокрема набуває дедалі більшої актуальності. Це, у свою чергу, потребує визначення пріоритетних напрямів проведення превентивних заходів із забезпечення інформаційної та кібернетичної безпеки відповідно до загроз в інформаційній сфері.

Проте, за висновками експертів, чинна вітчизняна нормативно-правова база у сфері протидії кібератакам лише частково задовольняє потреби сьогодення та не завжди охоплює всі ключові елементи, необхідні для ефективної протидії кібератакам, зокрема, "деталізації правових норм щодо відповідальності за несанкціоноване втручання і несанкціоновані дії щодо державних електронних інформаційних ресурсів та інформаційно-телекомунікаційних систем об'єктів критичної інформаційної інфраструктури держави, диференціації відповідальності за вчинення таких протиправних посягань" [2].

Результати аналізу наукових публікацій. Проблемам кібербезпеки, протидії кібератакам кіберзлочинності, захисту об'єктів критичної інформаційної інфраструктури та захисту інформації зокрема були присвячені праці таких науковців і практиків, як К.І. Бєляков, В.М. Брижко, В.М. Бутузов, М.В. Гребенюк, М.В. Гуцалюк, М.Ю. Літвінов, А.І. Марущак, В.Г. Пилипчук, Н.А. Ткачук та інших, проте питанням посилення ефективності протидії кібератакам та аналізу стану виконання рішень РНБО України щодо забезпечення кібербезпеки України, зокрема, розмежування підслідності розслідування кібератак доцільно приділити більше уваги.

Метою статті є обгрунтування необхідності "деталізації правових норм щодо відповідальності за несанкціоноване втручання та несанкціоновані дії щодо державних електронних інформаційних ресурсів та інформаційно-телекомунікаційних систем об'єктів критичної інформаційної інфраструктури держави, диференціації відповідальності за вчинення таких протиправних посягань" та визначення стану виконання рішення РНБО України з цих питань.

Виклад основного матеріалу. Варто зазначити, що питання забезпечення кібербезпеки перебувають у постійному полі зору РНБО України. З цієї проблематики було прийнято низку рішень, що були введені у дію Указами Президента України. Разом з тим, існують певні проблемні питання щодо імплементації цих рішень.

Основну роль у протидії кібератакам відіграють підрозділи Служби безпеки України, зокрема Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ, який забезпечує кібернетичну та інформаційну безпеку України. Але для більш ефективної протидії кібератакам необхідно, серед іншого, отримання нових законодавчо-визначених інструментів протидії кібернетичним та інформаційним впливам [3].

На ефективність протидії кібератакам через несанкціоноване втручання в роботу державних інформаційних ресурсів, об'єктів критичної інфраструктури впливає відсутність кримінально-процесуальних важелів впливу Служби безпеки України на сферу таких злочинів, які наносять значну шкоду державній безпеці України. Одним із таких важелів є розмежування підслідності.

Відповідно до положень частини другої статті 8 Закону України "Про основні засади забезпечення кібербезпеки України", заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів здійснюються Національною поліцією України. Крім того, стаття 216 Кримінального процесуального кодексу України відносить розслідування злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виключно до підслідності слідчих підрозділів вказаного правоохоронного органу.

Таким чином, потребує вирішення питання щодо розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені стосовно державних та інших інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури та інших об'єктів.

Варто зазначити, що з кримінально-правової точки зору посягання на інформаційно-телекомунікаційні системи суспільного та державного значення мають більший ступінь суспільної небезпеки порівняно з інформаційною безпекою особи. Відповідно, і міра кримінальної відповідальності має бути суворішою.

Іноземний досвід свідчить, що виправданим є підхід, коли посягання на державні інформаційно-телекомунікаційні системи, зважаючи на їх значення для суспільства, повинні тягти за собою спеціальну відповідальність [4].

Покладання на Службу безпеки України в установленому порядку завдань з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, було визначено в Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [1].

10 липня 2017 року Рада національної безпеки і оборони України, розглянувши комплекс проблем у сфері забезпечення кібербезпеки, пов'язаних із наслідками здійснених масованих кібератак на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури, прийняла рішення, затверджене Указом Президента України від 30 серпня 2017 року № 254/2017 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введене в дію Указом Президента України від 13 лютого 2017 року № 32, в якому Кабінету Міністрів України доручено в шестимісячний строк підготувати за участю Служби безпеки України та подати в установленому порядку на розгляд Верховної Ради України законопроект щодо розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

Планом заходів на 2018 рік з реалізації Стратегії кібербезпеки України, затвердженим розпорядженням Кабінету Міністрів України від 11 липня 2018 року № 481-р, передбачалося підготувати пропозиції щодо врегулювання на законодавчому рівні розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

На виконання цього рішення Адміністрацією Держспецзв'язку спільно зі Службою безпеки України наприкінці березня 2018 року підготовлено проект Закону України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної

інформаційної інфраструктури", який було подано до Верховної Ради України і зареєстровано 16 квітня 2018 року (реєстр. № 8304).

Варто також зазначити, що народним депутатом України Семенухою Р.С. було подано законопроект "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за злочини, вчинені у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, та відповідальності за пошкодження телекомунікаційних мереж" (реєстр. № 8304-1).

Альтернативним законопроектом було запропоновано запровадити кваліфіковані види таких злочинів, як несанкціоноване втручання в роботу інформаційно-телекомунікаційних систем, несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в інформаційно-телекомунікаційних системах, несанкціонована зміна, знищення або блокування комп'ютерної інформації, перешкоджання роботі інформаційно-телекомунікаційних систем, передбачивши підвищену відповідальність за вказані дії, якщо вони вчинені стосовно об'єктів критичної інформаційної інфраструктури (зміни до статей 361, 361-2, 362, 363, 363-1 КК України); віднести розслідування злочинів, вчинених стосовно об'єктів критичної інформаційної інфраструктури, до підслідності Служби безпеки України (зміни до частини 2 статті 216 КПК України); уточнити об'єктивні ознаки такого адміністративного правопорушення, як порушення правил охорони та порушення телекомунікаційних мереж, і посилити відповідальність за його вчинення (зміни до статті 147 КУпАП).

7 листопада 2018 року Комітет Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності рекомендував Верховній Раді України прийняти в першому читанні за основу проект Закону України (реєстр. № 8304), суб'єктом права законодавчої ініціативи якого є Кабінет Міністрів України, а проект Закону України (реєстр. № 8304-1), суб'єктом права законодавчої ініціативи якого є народний депутат України, відхилити.

При цьому експерти Головного науково-експертного управління Апарату Верховної Ради України зазначили, що за результатами розгляду в першому читанні цей законопроект доцільно повернути суб'єктам права законодавчої ініціативи на доопрацювання з урахуванням висловлених зауважень та пропозицій.

Варто також наголосити, що питання розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені стосовно державних та інших інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідно посилення кримінальної відповідальності за вчинення таких злочинів уже було вирішеним. Так, на початку 2014 року КК України доповнено статтями 361-3, 361-4 та 362-1 відповідно до Закону України від 16 січня 2014 року №721-VII "Про внесення змін до Закону України "Про судоустрій і статус суддів" та процесуальних законів щодо додаткових заходів захисту безпеки громадян» [5], який втратив чинність на підставі Закону України від 28 січня 2014 року № 732-VII "Про визнання такими, що втратили чинність, деяких законів України" [6] та Закону України від 23 лютого 2014 року № 767-VII "Про внесення змін до деяких законодавчих актів України щодо припинення норм законів, схвалених 16 січня 2014 року" [7].

На офіційному сайті Верховної Ради України в тексті КК України ці статті присутні з коментарем “Статтю виключено на підставі Закону № 767-VII від 23.02.2014” [7].

Висновки.

На сьогодні залишається невиконаним стратегічне завдання щодо розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об’єктів, а також не здійснено відповідне розмежування підслідності таких злочинів, що визначено в підпункті 4.4 Стратегії кібербезпеки України, уведеної в дію рішенням Ради національної безпеки і оборони України від 27 січня 2016 року.

Це є свідченням того, що виконання окремих важливих рішень РНБО України, присвячених кібербезпековим технологіям, відбувається повільно, із значним порушенням визначених строків виконання. Законопроекти, пов’язані з питаннями захисту кіберпростору держави, не розглядаються Верховною Радою України протягом багатьох місяців, а то й років.

Крім того, законодавство щодо кібербезпеки країни також не є досконалим. Зокрема в Україні на сьогодні законодавчо, на жаль, не визначено сфер відповідальності між різними державними та правоохоронними органами. Закон України “Про основні засади забезпечення кібербезпеки України”, з одного боку, визначає базові поняття та передбачає відповідальність керівників організацій за можливі кіберінциденти, з іншого – за кібербезпеку відповідають усі державні структури: Кабмін, Нацполіція, СБУ, Держспецзв’язку та Міноборони, НБУ, але виключно абстрактно.

Також у рамках розбудови інституційного забезпечення кібербезпеки необхідно врегулювати організаційно-правові засади, на яких має бути побудована кібербезпека об’єктів критичної інфраструктури, оскільки Закон України “Про основні засади забезпечення кібербезпеки України” не визначає переліку таких об’єктів. Крім того, ще й досі не розроблені підзаконні акти, які мають регулювати нормативи кібербезпеки на об’єктах критичної інфраструктури.

З огляду на викладене доцільно в рамках виконання Концепції розвитку сектору безпеки і оборони України прискорити схвалення законопроектів, пов’язаних із забезпеченням кібербезпеки України, зокрема законопроектів “Про критичну інфраструктуру та її захист” (реєстр № 10328) і “Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури” (реєстр № 8304).

Використана література

1. Про рішення Ради національної безпеки і оборони України від 27.01.16 р. “Про Стратегію кібербезпеки України”: Указ Президента України від 05.05.16 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016

2. Захист демократичних цінностей і дотримання прав людини у діяльності спецслужб: Рекомендації VI Міжнародної конференції, Київ, 24 квітня 2013 року. URL: http://ssu.kmu.gcv.ua/sbu/doccatalog/docinnent?id=l17284

3. Інформаційна та кібербезпека в сучасному світі: досвід СБУ. URL: https://ua-news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-v-suchasnomu-sviti-dosvid-sbu

4. Пашнєв Д.В. Необхідність спеціальної кримінально-правової охорони критичної інформаційної інфраструктури. *Вісник Кримінологічної асоціації України*. 2014. № 6. С. 73-82.

5. Про внесення змін до Закону України "Про судоустрій і статус суддів" та процесуальних законів щодо додаткових заходів захисту безпеки громадян: Закон України від 16.01.14 р. № 721-VII. *Голос України*. 2014. № 10.

6. Про визнання такими, що втратили чинність, деяких законів України: Закон України від 28.0114 р. № 732-VII. *Голос України*. 2014. № 19.

7. Про внесення змін до деяких законодавчих актів України щодо припинення норм законів, схвалених 16 січня 2014 року: Закон України від 23.02.14 р. № 767-VII. URL: https://zakon.rada.gov.ua/laws/show/767- 18#п 137

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~