Біленко А. О.,
студентка 2 курсу магістратури, 8 групи, Інституту прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого

ЗАХОДИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Ключові слова: кіберзлочини, кіберзлочинність, протидія кіберзлочинності, стан кіберзлочинності, динаміка кіберзлочинності, запобігання кіберзлочинності, заходи запобігання.

Анотація. У тезах розглянуто латентність та динамічність кіберзлочинності. Проаналізовано заходи запобігання кіберзлочинів.

Аннотация. В тезисах рассмотрены латентность и динамичность киберпреступности. Проанализированы меры предотвращения киберпреступлений.

Ключевые слова: киберпреступления, киберпреступность, противодействие киберпреступности, состояние киберпреступности, динамика киберпреступности, предотвращения киберпреступности, меры предупреждения.

Keywords: cybercrime, cybercrime, counteraction to cybercrime, state of cybercrime, dynamics of cybercrime, cybercrime prevention, prevention measures.

Summary. The theses consider the latency and dynamics of cybercrime. Measures to prevent cybercrime are analyzed.

В сучасних умовах розвитку суспільства бізнес-процеси, та, загалом, людське життя переходить у віртуальний простір. Глобалізація та впровадження інноваційних технологій в більшості галузей науки, політики, економіки, автоматизація процесів життєдіяльності, призвели до нівелювання кордонів і переплетення національних економік і національних інфраструктур країн світу, що, в свою чергу, призвело до проблем кібербезпеки. Постіндустріальна стадія розвитку людства вимагає переосмислення й уточнення багатьох положень кримінологічної теорії, перегляду традиційних підходів до боротьби зі злочинністю. На сучасному етапі кримінологія проходить етап формування нової парадигми, зміни наукового світогляду, генерування ідей та упровадження інновацій [7, 169].

Кіберзлочини є специфічним видом кримінальних правопорушень у зв'язку із їх динамічністю та латентністю. Це поняття охоплює широкий спектр різноманітних злочинів, які можна поділити на дві основні групи: 1) злочини, спрямовані на вплив на комп'ютерні мережі або пристрої (вірусні атаки типу (DoS). 2) злочини, в яких використовуються комп'ютерні мережі які інструмент для здійснення злочинної діяльності (кіберштурм, фішинг, шахрайство) [1, с. 236].

В нашій державі на законодавчому рівні врегульовано питання боротьби, запобігання та протидії кіберзлочинності. Проте, нормативно-правова база потребує постійного вдосконалення у зв'язку із вже зазначеною особливістю вказаних злочинів – їх динамічністю та латентністю. Методологічною основою дослідження є твердження, що людський потенціал формується на основі стосунків усередині груп людей, які об'єднуються через спільні інтереси та підтримують неформальні контакти з метою взаємної вигоди та допомоги. Людський потенціал нерозривно пов'язаний з інституційними формаціями, буквально сформованими ними [8].

Так, на сьогодні, Законом України «Про основні засади забезпечення кібербезпеки України» визначені правові та організаційні засади забезпечення захисту у кіберпросторі, а також цілі, напрями, принципи державної політики у цій сфері; повноваження відповідних органів [2]. В суспільстві відбуваються інтенсивні процеси інформатизації та інтелектуалізації, прискореними тем-

пами формується інформаційне суспільство, особливістю якого є комп'ютеризація всіх сфер людського життя. Останнім часом комп'ютерні технології та комп'ютерні системи використовуються в більшості злочинів як засіб їх вчинення [9, с. 1297].

Водночас, розглядаючи питання запобігання кіберзлочинності в Україні заслуговує на увагу думка про те, що, окрім належного нормативно-правового регулювання, є ще три види заходів: загально-соціальний, спеціально-кримінологічний та індивідуальний заходи запобігання.

Запобігання кіберзлочинності на загально-соціальному рівні передбачає комплекс організаційно-управлінських, соціально-економічних, ідеологічних, виховних заходів, що будуть спрямовані на підвищення обізнаності населення щодо даної категорії злочинів та можливості боротьби з нею, належну організація діяльності правоохоронних органів та органів державної влади та місцевого самоврядування [3].

Спеціально-кримінологічне запобігання стосується безпосередньо діяльності органів Національної поліції України, зокрема їх превентивної діяльності. Так, основними заходами в цьому напрямі є розроблення відповідних інструкцій, положень, видання наказів, які б спрямовували та координували роботу органів та підрозділів Національної поліції України для підвищення ефективності їх роботи. Окрім того, до таких заходів належать моніторингові механізми перевірок органами поліції підприємств, установ та організацій, що провадять діяльність, пов'язану з використанням комп'ютерних технологій або наданням інформаційних послуг, з метою виявлення випадків використання нелегального (нерегламентованого) програмного забезпечення; притягнення до відповідальності уповноважених осіб таких підприємств, установ або організацій; встановлення посиленого контролю за обігом будь-яких технічних засобів, заборонених для використання у вільному обігу або використання яких є обмеженим (технічні засоби для негласного зняття інформації з каналів зв'язку, прослуховування, перехоплення кодованих сигналів, добору паролів тощо) тощо [4, с. 163-164].

Індивідуальні заходи запобігання кіберзлочинів – це діяльність, спрямована на виявлення осіб, які вчиняють або схильні до вчинення кіберзлочинів.

Окрім того, слід звернути увагу, що заходи щодо протидії та запобігання кіберзлочинності на сьогодні модернізуються. Так, проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів, зареєстрований під № 4004 01.09.2020 передбачає впровадження якісно нового рівня взаємодії правоохоронних органів та інтернет-провайдерів при здійсненні оперативно-розшукових заходів, застосуванні заходів забезпечення кримінального провадження, проведення негласних слідчих (розшукових) дій [5].

Виходячи з аналізу тексту законопроекту №4004, він містить вимогу, про зобов'язання провайдерів за власний рахунок встановлювати в своїх мережах технічні засоби для проведення негласних слідчих (розшукових) дій, доступу до інформації про зв'язок, абонента, отриманні та маршруті передачі інтернет-послуг, їх тривалості і змісті; а також вимогу щодо сприяння органам та оперативним підрозділам Національної поліції України [6, с. 205]. Зазначене, окрім іншого, сприятиме підвищенню ефективності розслідування кіберзлочинів, що позитивно впливати на зменшення кількості подібних злочинів в майбутньому.

Отже, виходячи із законодавчого врегулювання та практики запобігання кіберзлочинності в Україні, можна зробити висновок про те, що в нашій країні здійснюється ряд заходів, які мають позитивний вплив та такий специфічний вид злочинів як кіберзлочини, незважаючи на їх латентність. Водночас, визначення єдиної політики, принципів і методів запобігання кіберзлочинності, а також визначення системи інституцій та окреслення їм відповідних повноважень, спрямованих на боротьбу з кіберзлочинністю є потреба сучасного українського суспільства в рамках запобігання кіберзлочинності.

ЛІТЕРАТУРА:

1. Біленчук П. Д. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму / П. Д. Біленчук, Т. В. Обіход // Часопис Київського університету права. 2018. № 3. С. 235-239.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Кравцова М. О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. Юридичний науковий електронний журнал. 2014. № 5. С. 110–113. URL: http://lsej.org.ua/5_2014/5_2014.pdf

4. Кравцова, М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні / Марина Олександрівна Кравцова // Вісник Кримінологічної асоціації України. 2018. № 2 (19). С.155-166.

5. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів. Номер, дата реєстрації: 4004 від 01.09.2020. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

6. Таволжанський О. В. Сучасні реалії кіберпростору України// Забезпечення правопорядку в умовах коронакризи : матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р. / редкол.: В. Я. Тацій, А. П. Гетьман, Ю. Г. Барабаш, Б. М. Головкін. – Харків : Право, 2020. С. 203-208. URL: http://dspace.nlu.edu.ua/bitstream/123456789/18127/1/Tavolzhanskiy_203-208.pdf

7. Головкін Б.М. Теперішнє і майбутнє кримінології //Проблеми законності. Харків : Нац. юрид. ун-т імені Ярослава Мудрого. 2020. № 149. С. 168- 184.URL: http://plaw.nlu.edu.ua/article/view/200724/205532

8. Tsypko, Victoria, Kateryna I. Alieksieieva, Iryna A. Venger, Oleksii V. Tavolzhanskyi, Nataliya I. Galunets, & Alona V. Klyuchnik. « Information Policy of the Enterprise as the Basis for the Reproduction of Human Potential in the Structure of Public Social Interaction.» Journal of Advanced Research in Law and Economics [Online], 10.6 (2019): 1664-1672. Web. 6 Nov. 2020.

9. Ovcharenko, Mykola O; Tavolzhanskyi, Oleksii V; Radchenko, Tetiana M; Kulyk, Kateryna D; Smetanina, Nataliia / Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method /Tavolzhansky O. V.// V.Journal of Advanced Research in Law and Economics; Craiova Том 11, Изд. 4(50), (Summer 2020): 1296-1304.

Науковий керівник: к.ю.н., доц. О. В. Таволжанський