Лукашенко М. І.,
студентка 6 курсу, 5 групи,
Інституту прокуратури та кримінальної юстиції Національного юриидичного університету імені Ярослава Мудрого

ОСОБЛИВОСТІ ДЕТЕРМІНАЦІЇ КІБЕРЗЛОЧИННОСТІ

Ключові слова: кіберзлочинність, детермінація, причини та умови кіберзлочинів.

Анотація. Тези присвячені аналізу особливостей детермінації кіберзлочинності. Визначені детермінанти кіберзлочинності з урахуванням специфіки обговорюваної злочинної діяльності.

Ключевые слова: киберпреступность, детерминация, причины и условия киберпреступлений.

Аннотация. Тезисы посвящены анализу особенностей детерминации киберпреступности. Определены детерминанты киберпреступности с учетом специфики обсуждаемой преступной деятельности.

Keywords: cybercrime, determination, causes and conditions of cybercrime.

Summary. The theses are devoted to the analysis of the features of cybercrime determination. The factors of cybercrime are determined, taking into account the specifics of the discussed criminal activity.

Нинішня система знань, понять і категорій кримінології сформувалася у період індустріального розвитку суспільства і некласичної науки. Постіндустрі- альна 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 [1, 169].

Актуальність проблеми кіберзлочинності зростає все більше з урахуванням глобальної автоматизації установ, підприємств та організацій публічного та приватного характеру. Швидкий розвиток та щоденне використання інформаційних технологій, перетворення інформації у найважливіший ресурс життя визначає рух

людства до інформаційного суспільства. Інформаційна революція принесла нові ефективні можливості в життя людей, відкрила безпрецедентні перспективи: спрощений доступ до інформації, зробив можливим обробку великих обсягів інформації [2]. Цей вид злочинності поряд з такими поняттями як економічна злочинність, організована злочинність, корупція, легалізація злочинних доходів хоча і з'явився нещодавно, але міцно увійшов у понятійний апарат кримінологів і практичних працівників. Не так давно злочинам в кіберсфері на національному рівні приділялась незначна увага, вважалось, що кіберзлочинність може представляти реальну загрозу лише в далекому майбутньому, тепер майже ні в кого не виникає сумнівів, що частка кіберзлочинності в структурі злочинності України значно збільшилася [3, с. 81]

У системі суспільних відносин криміногенні та антикриміногенні явища і процеси взаємопов'язані та співвідносяться як діалектичні протилежності. Вони одночасно впливають на суспільну свідомість, однак відображаються, сприймаються та оцінюються мисленням по-різному.

Закономірно, що різноманітність різного роду втручань у роботу інформаційних систем, які призводять до порушення або припинення їх нормального функціонування, зумовлює постійний пошук релевантних механізмів захисту від несанкціонованого впливу на діяльність інфраструктури інформаційних технологій. За законами формальної логіки для того, щоб провадити ефективну роботу по боротьбі, запобіганню та попередженню певного виду злочинної активності, потрібно проаналізувати першопричини та умови, які сприяють розвитку такої діяльності, а отже – звернутися до детермінації.

З огляду на специфіку обговорюваного типу злочинної діяльності в науці виділяють комплекс чинників, які сформовані з урахуванням особливостей предмету злочинного посягання та безпосередньо засобів, способів та шляхів його вчинення. Традиційно, у механізмі детермінації кіберзлочинності можна умовно виділити такі групи чинників: соціальні, політичні, економічні, технологічні та психологічні [4, с. 259].

Соціальною передумовою вчинення кіберзлочинів є майже абсолютна комп'ютеризація суспільства, яка, на жаль, інколи не усвідомлюється пересічними громадянами, що робить їх вразливими перед злочинними посяганнями. Проте, аналізуючи найбільш гучні випадки кібератак у світі (наприклад, атака Stuxnet у 2008 році) можна дійти до висновку, що навіть провідні організації, оснащені найпотужнішими системами захисту, можуть стати жертвами кіберзлочинності.

Політичні чинники виявляються у недостатньому усвідомленні урядом можливих соціальних наслідків кіберзлочинності. У зв'язку з цим обмежуються бюджетні фінансування робіт зі створення правової, організаційної, технічної бази інформаційної безпеки держави та захисту прав і свобод громадян у віртуальному просторі [4, с. 260]. В цьому контексті також варто не забувати про відсутність кордонів інформаційного простору, що має своїм наслідком підвищення кількості кібератак політичного забарвлення. Яскравим прикладом із вітчизняного досвіду є атака 27 червня 2017 року, коли вірус невідомого походження, який згодом отримав назву «вірус Petya», атакував комп'ютерні системи сотень державних установ, підприємств та організацій. Урядова активність з боку світових лідерів у кіберпросторі, лобіювання інтересів поза територіальними і національними рамками інформаційної політики та організація і успішна діяльність транснаціональних злочинних угруповань, що «фахово» вузько спрямовано займаються кіберзлочинністю все це обумовлює необхідність виробленні рекомендацій щодо обрання напрямків і сфер видозміни [2, с. 159].

Економічні чинники кіберзлочинності мають дуалістичну природу і частково корелюються із суспільними чинниками. З одного боку економічний фактор проявляється у прибутковості кіберзлочинності [4, с. 260]. З іншого боку їх вплив виражається у розвитку електронної торгівлі, можливості відкриття банківських рахунків через Інтернет і здійснення опліпе-операцій, що не вимагають безпосереднього контакту з контрагентом, появі електронних грошей, що обумовлює зростання кількості кіберзлочинів в сфері торгівлі і операцій з кредитними картками, крадіжок персональних даних, паролів доступу [5, с. 114-115].

Технологічні чинники кіберзлочинності є наслідком бурхливого розвитку комунікаційних та інформаційних технологій, що робить їх все більш доступними для використання. В результаті ми маємо надзвичайно високий показник кількості активних корис-

тувачів комп'ютерних технологій, кожен з яких потенційно може використати здобутки прогресу для власних злочинних цілей.

Психологічні чинники зумовлені особливостями функціонування віртуального простору. У реальному світі існують певні стримувальні засоби, а у віртуальному – злочинці не можуть бачити своїх жертв, яких вони обрали для атаки. У зв'язку з цим у винних осіб є певне усвідомлення анонімності та відсутності безпосереднього ризику бути виявленим та притягнутим до кримінальної відповідалності [4, с. 261].

Додатково до детермінант кіберзлочинності можна віднести правовий та компетенційний чинники. Відсутність належного регулювання в національному законодавстві, складнощі зі тлумаченням та застосуванням норм, недостатній рівень співпраці національних правоохоронних органів з відповідними компетентними органами суб'єктів міжнародної спільноти – всі ці фактори є складовими правового чиннику. Сутність компетенційного чинника полягає у тому, що переважна частина складу правоохоронних органів належним чином не підготовлена до боротьби з новітніми видами злочинів, зокрема і кіберзлочинами.

ЛІТЕРАТУРА:

1. 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

2. Tavolzhanskyi, O.V. (2017). Osnovu derzhavnoi kiberpolituku Ukrainu: formuvannya ta realizatsiya. Naykovo-informatsyinui visnuk Ivano-Frankivskogo yniversutety prava imeni Korolya Danula Galutskogo: Seriya Pravo, 4. (16), 158–164 [In Ukrainian].

3. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах / О. В. Таволжанський // Журнал східноєвропейського права. 2016. № 31. С. 80-86. URL: http://dspace.nlu.edu.ua/bitstream/123456789/17724/1/Tavolzhanskyi_80-86.pdf (дата звернення: 11.11.2020).

4. Кримінологія / заг. ред. Б. М. Головкін. Харків: Право, 2020. 384 с.

5. Кравцова М. О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії / М. О. Кравцова // Юридичний науковий електронний журнал. 2014. № 5. С. 113-116. URL: http://www.lsej.org.ua/5_2014/32.pdf (дата звернення: 11.11.2020).

6. 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.

7. Головкін Б.М. Про детермінацію злочинності // Часопис Київського університету права. Київ: Інститут держави і права ім. В.М. Корецького НАН України. – 2020. – № 1. 274-280 с. URL: http://kul.kiev.ua//images//A/Chasopis/CHAS20_1.pdf

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