УДК 004.946.5.056

Юлія Вікторівна Гурзель,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: основні причини та методи боротьби

Розповсюдження комп'ютерних технологій та техніки, повсюдне існування телекомунікаційних мереж як полегшило, так і ускладнило сучасний інформаційний світ. Йдеться про створення безпечних умов використання віртуального простору, адже з кожним днем збільшується злочинність у всесвітній мережі. Більш того, розмах комп'ютеризації та рівень можливостей, які при цьому одержують зловмисники, й тенденція збільшення кількості злочинів у комп'ютерних інформаційних технологій становлять загрозу національній безпеці України. Поширення комп'ютерних вірусів, шахрайство, крадіжки коштів із банківських рахунків, викрадення персональної та комерційної інформації – це ще не весь перелік кіберзлочинів, оскільки з кожним днем їх кількість та різноманіття тільки збільшується.

Слід зазначити, що з приводу поняття кіберзлочинів в науці кримінального права досі триває дискусія, адже на національному рівні це поняття не має нормативного регулювання, проте цим терміном оперує Конвенція про кіберзлочинність (2001 р.) [1].

Боротьба з кіберзлочинністю неможлива без розуміння правового регулювання інформаційних мереж. Щоб це зробити, потрібно з'ясувати основні причини цього злочину. Ними зокрема є:

1. Головна причина кіберзлочинності – велика прибутковість; внаслідок окремих кіберзлочинів можна отримати великі гроші. Дослідження показує, що кіберзлочинність посідає третє місце після торгівлі наркотиками та зброєю за рівнем збагачення.

2. Соціальні чинники – зміни в суспільному житті, пов'язані із комп'ютеризацією, а також із формуванням інформаційного простору.

3. Технологічні причини – це ті, які проявляються в технічному просторі вчинення кіберзлочинів. Високопрофесійні хакери можуть обходити будь-який захист і замаскувати всі сліди вторгнення. Негатив-

ним чинником є також поширення вірусного ринку в Інтернеті, що дає можливість вчинити злочин навіть тим, хто не володіє комп'ютерними знаннями.

4. Політичні причини, що проявляються в недостатній компетентності уряду щодо можливих слідів кіберзлочинності. Досить мало уваги приділяється правовому регулюванню комп'ютерної системи, яка в порівнянні з іншими деградує у своєму технічному розвитку.

Сьогодні є безліч злочинів, які не знайшли своє місце в законодавстві, тому слід удосконалювати кібербезпеку, залучати до цього спеціалістів, також потрібно не забувати про міжнародне співтовариство, що сприятиме посиленню безпеки.

Кіберзлочинність є один із найпоширеніших видів суспільно небезпечних діянь. Зокрема соціальна небезпека інтернет-піратства постійно зростає. Порушення авторських прав – дія, спрямована на незаконне використання об'єктів інтелектуальної власності, що належать іншим особам. За даними дослідження Асоціації виробників програмного забезпечення (BSA), на 2011 р. рівень піратства в Україні становив майже 85% [2].

Згідно із чинним законодавством, порушення авторського права і суміжних прав чітко визначений як кримінальний злочин, передбачений ст. 176 Кримінального кодексу України, згідно з якою максимальний штраф становить від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або такий злочин карається виправними роботами на строк до двох років або позбавлення волі на той самий строк [3].

Що ж потрібно робити для захисту у мережі?

1. Встановіть надійний пароль, не коротший за 12 символів, не зберігайте його у браузері. Використовуйте різні паролі для кількох облікових серверів.

2. Виходьте зі своїх профілів, якщо ви користувались публічним комп'ютером.

3. Не завантажуйте файли із ненадійних сайтів.

4. Прогляньте і налаштуйте приватність своїх акаунтів у соціальних мережах.

5. Використовуйте двофакторну автентифікацію.

6. Не ходіть по підозрілих посилань

7. Довіряйте антиспам-фільтрам електронної пошти.

Як правило, вони фільтрують практично всі листи, обманом заманює вас на той чи інший хакерський сайт.

8. Встановіть комплексну систему захисту. Сьогодні актуальні так звані «комплексні системи захисту», які включають в себе антивірус, файрволл, антиспам-фільтр і ще пару-трійку модулів для повного захисту вашого комп'ютера.

9. Робіть покупки тільки в перевірених онлайн-магазинах.

10. Користуйтеся ліцензійним програмним забезпеченням [4].

Зважаючи на вищесказане, можна дійти висновку, що кіберзлочинність набула популярності саме у XXI ст., коли зросла модернізація технологій та суспільства. Звичайно, вживаються заходи щодо боротьби із цим злочином, але їх недостатньо. Тому варто приділяти більше уваги цій проблемі, розробляти нові методи боротьби, що дадуть набагато більше позитивних результатів, а також покращити систему захисту у соціальних мережах.

Список бібліографічних посилань

1. Конвенція про кіберзлочинність : від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.09.2018).
2. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // Ресурсний центр гурт : сайт. 03.10.2016. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення: 30.10.2019).
3. Кримінальний кодекс України: чинне законодавство зі змінами та допов. Станом на 1 верес. 2019 року : офіц. текст. Київ : Паливода А.В., 2019. 264 с.
4. Українська Антипіратська Асоціація : офіц. сайт. URL http://apo.kiev.ua/index.php (дата звернення: 30.10.2019).

Одержано 01.11.2019