УДК 004.946.5.056

Роман Андрійович Івасечко,
студент 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність як один із найбільш прогресивних видів злочинів сучасності

Свого часу Білл Гейтс зазначав, що в майбутньому на ринку будуть присутні тільки два види компаній: ті, хто в Інтернеті і ті, хто вийшов з бізнесу.

Можна сказати, що це майбутнє вже настало, адже бізнес масово починає «переходити» у Всесвітню павутину, і поряд із цим виникає і масово розвивається кіберзлочинність, однією з причин якої є величезний обіг коштів у даній сфері суспільних відносин.

З огляду на те, що проблема кіберзлочинності на сучасному етапі розвитку України набуває популярності та становить загрозу інформаційному суспільству, вона вже отримала відображення у нормативно – правових актах національного та міжнародного рівнів. Зокрема, 15 березня 2016 року Президент України видав Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». У складі Ради національної безпеки створено робочий орган – Національний координаційний центр кібербезпеки.

Г. М. Чернишов стверджує, що кіберзлочинність у сучасних умовах інформаційного суспільства та глобальної комп'ютеризації є однією з найбільших загроз світовій безпеці. Кіберзлочинність – явище, яке виражається у системі злочинів, вчинених у кіберпросторі з використанням та/або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку. Кіберзлочинність – злочини, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення [1].

Станом на сьогодні кіберзлочинність є одним з найбільш активно прогресуючих видів злочинності. Великими темпами розвиваються нові види кіберзлочинів, а також суттєво збільшується їх кількісне

значення та територія поширення. Для прикладу, Н. Міщук зазначає, що за даними фахівців США, розмір збитків від кіберзлочинності кожного року зростає в середньому на 35% порівняно з попереднім. Однією з причин такого стрімкого розвитку є саме кількість коштів, яку можна отримати при вчиненні кіберзлочину. Середня кількість збитків від кіберзлочину у світі становить приблизно 560 тисяч доларів, тоді як при звичному пограбуванні банку – приблизно 20 тисяч доларів [2, с. 174].

Як вже було сказано, кібернетична злочинність посягає на банківські рахунки як компаній чи організацій, так і пересічних громадян. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. Чинниками, які сприяють зростанню кіберзлочинів є розвиток та удосконалення ІТ-технологій, значна географія для скоєння злочинів, недостатня теоретична та практична підготовка працівників органів внутрішніх структур та недосконаліть вітчизняного законодавства [3].

Суспільну небезпечність кіберзлочинів та актуальність цієї проблеми ілюструє таке явище, як кібератака. Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення таких цілей: порушення конфіденційності, доступності електронних інформаційних ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [4].

Кібератаки, в силу своєї специфіки, дуже часто спрямовані на автоматизовані та інформаційні системи, що мають державне значення. прикладом цього можуть слугувати відомі кібератаки на енергетичні компанії України 23 грудня 2015 року, коли зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України, або кібератака 17–18 грудня 2016 року, коли була виведена з ладу підстанція «північна» енергокомпанії «Укренерго», що мало наслідком залишення без струму споживачів певних районів Києва.

Серед основних помилок користувачів виокремлюються такі як: використання одного і того ж паролю у кількох облікових записах, надсилання паролів чи даних банківських карток незахищеними каналами зв'язку, невикористання Proxy-сервісів або VPN-сервісів у момент

підключення до спільних безкоштовних точок WiFi-доступу до мережі Інтернет, в ході якої особисті дані користувача можуть вилучені сторонніми особами тощо.

На думку Г. М. Чернишова, враховуючи стрімкий розвиток комп'ютерних та Інтернет-технологій, залежність всіх сфер суспільства від їх функціонування, є доцільним внесення змін до КК України та доповненням певними статтями [5].

З огляду на це, можемо підсумувати, що кіберзлочинність є одним із найбільш прогресивних видів злочинності на сучасному етапі розвитку суспільства, що породжено значним поширенням використання мережі Інтернет у різних сферах суспільного життя та низькою захищеністю персональних даних користувачів Всесвітньої павутини.

Список бібліографічних посилань

1. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. Вип. 3 (24). С. 158–162.
2. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету*. 2014. № 51. С. 173–179.
3. Некрасов В. Легкие деньги: Украина превращается в Мекку для киберпреступников // Экономическая правда : сайт. 28.03.2016. URL: https://www.epravda.com.ua/rus/publications/2016/03/28/587004/ (дата звернення: 29.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
5. Чернишов Г. М Кібершахрайство: визначення та кримінологічні показники. *Порівняльно-аналітичне право*. 2018. № 5. С. 318–321.

Одержано 01.11.2019