УДК 343:004.056.53(477)

Яремко М.О

здобувач ступеня освіти бакалавр, Вінницький державний педагогічний університет імені М. Коцюбинського

СУЧАСНІ ТЕНДЕНЦІЇ ТА НАПРЯМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

В сучасних умовах інформаційні технології стрімко розвиваються, вони впроваджуються в усі сфери життєдіяльності людей. Використання сучасних персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних мереж забезпечило кожній людині можливості доступу до інформації, що зберігається у відповідних банках даних незалежно від доби і місцезнаходження абонента. У зв'язку з чим і з'явився такий вид злочинності як «кіберзлочинність».

Кіберзлочинність – це економічний злочин, скоєний з використанням обчислювальної техніки та мережі Інтернет, інформаційний простір, що моделюється за допомогою комп'ютера, в якому існують визначені об'єкти або символьне уявлення інформації – місце, де діють комп'ютерні програми і переміщуються дані [1].

В Україні до кіберзлочинів відносять:

1. порушення авторського права і суміжних прав;
2. шахрайство;
3. незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення;
4. ухилення від сплати податків, зборів (обов'язкових платежів);
5. ввезення, виготовлення, збут і розповсюдження порнографічних предметів;
6. незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю.

Об'єктом кіберзлочинів може стати будь-який користувач інтернету.

Найпоширенішими видами таких злочинів є:

•Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також, із персональних комп'ютерів (або безпосередньо через програми віддаленого доступу, «боти», «трояни»);

•Фітинг – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою, нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі;

•Онлайн-шахрайство - несправжні інтернет-аукціони , інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

•Вішинг – вид кіберзлочинів, у якому в повідомленнях містяться прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки;

•Піратство – незаконне розповсюдженні в Інтернеті інтелектуальної власності дані [2].

В сучасних умовах глобалізації значно зростають уразливості інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури.

Джерелами кіберзагроз можуть бути міжнародні злочинні групи хакерів, окремо підготовлені злочинці в сфері інформаційних технологій, іноземні державні органи та інші силові структури.

Кіберзлочинність, яка зупиняє мережі або перешкоджає бізнесу, що надає програмне обслуговування своїм клієнтам, називається атакою відмови в обслуговуванні.

Кіберзлочинність, яку використовує зловмисник за допомогою комп'ютера для вчинення інших злочинів, може передбачати використання комп'ютерних програм або мереж для розповсюдження шкідливого

програмного забезпечення, незаконної інформації чи незаконних зображень.

Іноді кіберзлочинці проводять відразу обидві категорії кіберзлочинів. Вони можуть спершу націлити комп'ютери на віруси. Потім використовувати їх для розповсюдження зловмисного програмного забезпечення на інші або по всій мережі.

Слід зазначити, що стрімкий розвиток інформаційних технологій постійно генерує нові види послуг. Це, в свою чергу, змушує злочинців удосконалювати свої здібності і знаходити нові способи незаконного заробітку в кіберпросторі.

До основних завдань у системі кібернетичної безпеки України належить:

- Протидія кіберзлочинності;
- Кіберзахист об'єктів критичної інформаційної інфраструктури;
- Забезпечення кібербезпеки у воєнній сфері та сфері оборони;
- Реагування на кіберзагрози державного суверенітету в кіберпросторі [3].

За останні п'ять років рівень кіберзлочинності в Україні виріс у 2,5 рази. Найбільше атак здійснюється на об'єкти банківської інфраструктури.

У 2017 році Україна стала жертвою шкідливої програми «Petya», тоді вірус блокував комп'ютерні системи компаній, вимагаючи за розблокування 300 доларів у біткойнах. Вірус поширювався електронною поштою, однак експерти не виключають, що він також циркулює всередині мережі. Зокрема, хакерська атака в Україні здійснювалась через програму для звітності та документообігу «M.E.doc».

Найбільш уразливими виявились українські компанії та відомства. Серед постраждалих – уряд України, національна пошта, метрополітен Києва, міжнародний аеропорт «Бориспіль», Чорнобильська АЕС, а також низка ЗМІ, банків, комерційних структур. Тоді вірус показав абсолютну неготовність українських державних органів та бізнесу до кібератак, це

стало причиною втрати інформаційних даних.

Більшість кіберзлочинів розцінюють як шахрайство, за яке відповідно до Ст.199 КК України, передбачено кримінальну відповідальність.

5 жовтня 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції. Метою створення Кіберполіції в Україні було реформування та розвиток підрозділів МВС України, зменшення кількості вчинених кібершахрайств та захист персональних даних у мережі [4].

У травні 2018 року набув чинності закон «Про основні засади забезпечення кібербезпеки України»

Документ визначає повноваження і обов'язки державних та приватних установ, організацій та громадян у сфері кібербезпеки, та визначає базові терміни, які з’явилися в українському законодавстві вперше. Наприклад, кіберзагроза, кібершпигунство чи кіберзлочинність[5].

Тому, щоб вберегти себе від кіберзлочинності, потрібно:

- Не надавати нікому персональні дані, паролі та коди-підтвердження з SMS для операцій з картками;
- Не заходити на невідомі сайти та скачувати з них сумнівні файли;
- Створювати надійні паролі та періодично їх змінювати, адже запорука надійного Інтернету – надійний пароль;
- Встановлювати антивірусні програми, які повинні перевіряти посилання, до того як користувач перейде за ним.

Отже, незважаючи на всі заходи боротьби з кіберзлочинністю держава має переглянути усі існуючі методи та активно розробляти нові, що принесуть більшу користь та надійний захист від кіберзлочинності.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА:

1. Кіберполіція [Електронний ресурс]. – Режим доступу: https://cyberpolice.gov.ua
2. Кіберзлочинність у всіх його проявах: види, способи боротьби та наслідки [Електронний ресурс]. – Режим

доступу:https://www.gurt.org.ua/articles/34602/

3. Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2. С. 276-282. URL: http://nbuv.gov.ua/UJRN/muvnudp_2018_1-2_46 (дата звернення: 29.06.2021)
4. Офіційний веб-сайт «Суспільне- Новини» [Електронний ресурс]. – Режим доступу: https://suspilne.media/65849-kiberzlocinnist-v-ukraini-za-5-rokiv-zrosla-u-ponad-dva-razi /
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017р. . № 2163-VIII. Дата оновлення: 24.10.2020. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення:29.06.2021).

УДК 330.341

Бойко В.О.

здобувач ступеня доктор філософії кафедри права і публічного управління Вінницького державного педагогічного університету імені М.Коцюбинського

ІННОВАЦІЙНИЙ ПОТЕНЦІАЛ ПІДПРИЄМСТВА ЯК НЕОБХІДНИЙ КОМПОНЕНТ ДЛЯ ЕФЕКТИВНОГО ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ

Сучасний етап розвитку світової економіки характеризується посиленням конкуренції і зростаючим впливом інноваційної діяльності на збільшення конкурентоздатності підприємств та темпи економічного розвитку. На світовому ринку продукти інтелектуальної діяльності мають більш високу вартість у порівнянні з іншими видами продукції. Тому зумовлюється необхідність створення умов для впровадження та використання в процесі здійснення комерційної діяльності інновацій та