УДК 343.34

Марків С. І.
викладач кафедри кримінального
права та процесу ЮФ ТНЕУ

КІБЕРЗЛОЧИННІСТЬ. НОВА КРИМІНАЛЬНА ЗАГРОЗА

Неможливо уявити сучасне життя без використання цифрових технологій, електронно-обчислювальних машин чи засобів комунікації. Майже усі найважливіші функції в сучасному суспільстві так чи інакше пов'язані з комп'ютерами чи комп'ютерними мережами. Постійно зростає кількість людей, які отримують доступ до всесвітньої мережі Інтернет. Сьогодні мати комп'ютер, смартфон, планшет з доступом до глобальної мережі вже не розкіш, а необхідність. Необмежений доступ до інформації, можливість вільної комунікації між країнами, та навіть континентами, спосіб для проведення банківських і торгових операцій – все це окремий світ, можливості якого неосяжні. Проте, як і в реальному світі, тут трапляються злочини – кіберзлочини.

Отримуючи доступ до інтернету, пересічний користувач залишає за собою сліди, інформацію, яка і стає об'єктом злочину. Номера телефонів, персональні дані, банківські рахунки, номера платіжних карток, це далеко не весь список всього чим прагнуть заволодіти зловмисники. Після ратифікації Україною Конвенції про кіберзлочинність від 7 вересня 2005р. такі суспільно-небезпечні діяння прийнято називати кіберзлочиномі.[1].

Сьогодні в Україні кіберзлочинність регулюється наступними нормативно-правовими акти: Кримінальний кодекс України, Конвенція про кіберзлочинність та Законом України "Про ратифікацію конвенції про кіберзлочинність". У Кримінальному кодексі України кіберзлочини як суспільно небезпечні діяння і закріплені у розділі "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". Розслідування такого виду злочинів неможливе без використання комп'ютерних технологій для відшукання, фіксування та вилучення слідів в електронній формі.

Найбільш розповсюдженою є класифікація кіберзлочинів на агресивні та неагресивні. До першої групи належать: кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає: кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм.[2].

Кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету (шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.), та нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям (злочини передбачені Розділом XVI Кримінального кодексу України). Найчастіше з використанням комп'ютера

та Інтернету вчиняються такі традиційні злочини: порушення авторського права і суміжних прав; шахрайство; незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів); ввезення, виготовлення, збут і розповсюдження порнографічних предметі; незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю [2]. Отже, можна стверджувати, що кіберзлочин – це передбачене кримінальним кодексом суспільно небезпечне діяння для скоєння якого застосовуються комп'ютерні технології та використовується глобальна мережа Інтернет.

Такий вид злочинності набуває все більшої популярності через свою специфіку. Дані злочини є доступними, їх можна вчиняти на великій відстані від об'єкту, і саме головне, що при проведенні слідчих дій доволі важко виявити та вилучити інформацію, яку можна розцінювати у якості доказу. Також не можна забувати, що це неймовірно прибутковий вид злочинної діяльності, успіх якої не потребує великого ризику.

Для скоєння злочину кіберзлочинці з кожним днем придумують все новіші та заплутаніші схеми. Від найпростіших виманювань цінностей у людини, коли вона добровільно перераховує кошти зловмисникам, до крадіжок бази зарплатних рахунків співробітників компанії чи установи для подальшого перепродажу, або проникнення в комп'ютерну мережу та виведення з ладу промислових об'єктів. Написання та розповсюдження вірусних та троянських програм, які потрапляючи на комп'ютер чи телефон починають слідкувати за їхнім власником, збирати та передавати інформацію про нього і призводить до небезпечних наслідків. Суб'єктом злочину може стати будь-хто, навіть цього не підозрюючи.

Найпоширинішими 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, або через програми віддаленого доступу, «трояни», «боти»).

Фішинг – 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.

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

Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті.

Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного TV.

Соціальна інженерія – технологія управління людьми в Інтернет-просторі.

Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення.

Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

Рефайлінг – незаконна підміна телефонного трафіку. [3].

Україна – не виняток, від дій кібершахраїв у 2016 році втрати українців склали 339,2 млн грн, за даними Української міжбанківської асоціації членів платіжних систем ЕМА за рік рівень кіберзлочинців із застосуванням вішингу (дзвінки клієнтам банку з метою отримати персональні дані платіжних карт) зріс у 5,3 рази і склав 275,5 млн. грн., в той же час втрати користувачів платіжних карток від шахрайських дій в Інтернеті збільшилися в 2 рази і склали 63,7 млн. грн., середня сума, яку шахраї збирали у власників карток склала 1403грн. Кількість виявлених фішингових сайтів, які збирали інформацію про користувачів становить понад 170.[4]. І з кожним роком ці цифри зростають, незважаючи на посилення боротьби з кіберзлочинцями ріст кіберзлочинів навпаки збільшується. Можна припустити, що з такими темпами розвитку в недалекому майбутньому кіберзлочинність переросте у щось більше і буде проблемою №1 у світі, більшою ніж тероризм та екстримізм.

Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Закони повинні складатись і відповідати сучасному рівню розвитку технологій. Необхідним є створення відповідних служб та їх тісної взаємодії з правоохоронними органами для належної боротьби з кіберзлочинністю. Важливим є безумовно і розвиток міжнародної співпраці в цій галузі.

ЛІТЕРАТУРА:

1. Конвенція про кіберзлочинність. Конвенція ратифікована із застереженнями і заявами Законом №2824-IV від 7.09.2005 ВВР 2006 №5-6 ст.7
2. Кримінологія: Загальна та Особлива частини Навчальний посібник. - Х.: Право, 2014. - 513 с.
3. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс]. – Режим доступу: http://gurt.org.ua/articles/34602/
4. Кіберзлочинність не спить - як не потрапити у тенета аферистів [Електронний ресурс]. – Режим доступу: http://news.finance.ua/ua/news/-/395023/kiberzlochynnist-ne-spyt-yak-ne-potrapyty-v-siti-aferystiv

Муравська (Якубівська) Ю. Е.
к.е.н., доцент, доцент, доцент кафедри
економічної безпеки та фінансових
розслідувань ЮФ ТНЕУ

ФОРМУВАННЯ ПОНЯТІЙНОГО АПАРАТУ У СФЕРІ КІБЕРБЕЗПЕКИ: ІНОЗЕМНИЙ ДОСВІД ТА НОРМАТИВНО-ПРАВОВА РЕГЛАМЕНТАЦІЯ

На сьогодні існує розгалужена система термінів, які окреслюють безпекове поле «ІТ-простору», однак гострою залишається питання їх нормативного формулювання, насамперед власне категорії «кіберпростір».