Микитчик Андрій Васильович,
т.в.о. завідувача кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ, кандидат юридичних наук

КРИМІНОЛОГІЧНІ ОСОБЛИВОСТІ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Анотація. Розглядаються актуальні питання які пов'язані з дослідженням кримінологічної характеристики кіберзлочинності в Україні, визначаються сучасні тенденцій даного виду злочинності, а також окреслюються ключові характерні ознак які їй притаманні.

Ключові слова: злочинність, кіберзлочинність, шахрайство, причини і умови, заходи запобігання.

Summary. The urgent issues related to the study of the criminological characteristics of cybercrime in Ukraine are considered, the current trends in this type of crime are determined, and the key characteristics that are inherent to it are outlined.

Keywords: criminality, cybercrime, fraud, causes and conditions, prevention measures.

На сьогоднішній день кожна держава світу ставить перед собою пріоритетну мету щодо створення інформаційного суспільства на основі широкого запровадження телекомунікаційних технологій.

У той же час, разом з розвитком інформаційного простору необхідно активізувати зусилля суспільства щодо його захисту від злочинних посягань, сукупність яких вже має свою власну, відому у всьому світі назву – кіберзлочинність. Вона встигла набути широкого поширення і в сучасних умовах становить одну з найбільш небезпечних загроз для суспільства.

Так, згідно з офіційними даними, щодня в інформаційному кіберпросторі з'являється від 90 до 150 тисяч шкідливих програм. При цьому злочинці все частіше використовують нові способи зараження комп'ютерів шкідливими програмами, які дозволяють отримувати незаконну вигоду. Серед найбільш поширених кіберзагроз є: спам, фішинг і мережеві атаки на інфраструктуру бізнес-організацій, включаючи цільові і DDos-атаки. Найчастіше інциденти в області IT-безпеки призводять до втрати даних, що стосуються інтернет-платежів (25 %), інтелектуальної власності (13 %), клієнтських баз (11 %), інформації про співробітників (10 %).

Близько 70 % інтернет-користувачів хоча б один раз стикалися з проявами шахрайства в мережі, і не менше 10 % з таких осіб, що використовують мобільні телефони і смартфони, постраждали від телефонних шахраїв. Зокрема, у 2018 році Департаментом кіберполіції Національної поліції України виявлено 6 тис. кримінальних правопорушень, з них 680 – у сфері приватного контенту, 2398 – у

сфері платіжних систем, 1598 – у сфері Е-комерції та 1325 у сфері кібербезпеки[1].

Стрімкому розвитку кіберзлочинності сприяє неготовність сучасного суспільства до запровадження ефективного запобіжного механізму. Кримінологічна наука досі не має у своєму розпорядженні достовірних відомостей про стан, рівень і структуру даної злочинності, а в теорії кримінального права і в правозастосовній практиці відсутня єдність поглядів щодо кримінально-правової оцінки кіберзлочинів. У зв'язку з цим значна частина суспільно небезпечних проявів кіберзлочинності залишається за межами заходів кримінально-правового реагування, що є сприятливим підґрунтям для її самодетермінації. Відповідно цим і обґрунтовується актуальність і необхідність розробки ефективних заходів запобігання кіберзлочинності.

Відповідно кіберзлочинність необхідно розглядати в якості самостійного виду злочинності, що виділяється на основі обов'язкової присутності в складі злочину таких ознак об'єктивної сторони, як засіб або знаряддя, в якості яких виступає шкідлива комп'ютерна програма або програмно-технічний засіб, підключений до комп'ютерної мережі або мобільного оператора зв'язку. Причому тісний взаємозв'язок даних злочинів з комп'ютерними та інформаційними видами злочинності прослідковується тільки в деяких її проявах, в основному пов'язаних з несанкціонованим доступом до комп'ютерної інформації, створенням і розповсюдженням шкідливих комп'ютерних програм. Особливістю кіберзлочинності є застосування злочинцями прийомів і методів, які передбачають що для досягнення злочинного результату використовуються шкідливі комп'ютерні програми або програмно-технічні засоби в якості знаряддя чи засобу вчинення злочину. Саме це надає зазначеним злочинам унікальні властивості, не характерні для інших видів злочинів.

Отже, до кіберзлочинів необхідно зараховувати тільки ті злочини, механізм вчинення яких передбачає обов'язкове використання програмно-технічних засобів і шкідливих комп'ютерних програм не раніше, ніж на стадії замаху на вчинення злочину, тобто коли суб'єкт злочину приступає до безпосереднього виконання об'єктивної сторони складу злочину. Причому в таких злочинах програмно-технічний засіб і шкідлива комп'ютерна програма може використовуватися і на стадії готування до злочину, але в обов'язковому порядку її використання повинно бути передбачено ще і в процесі вчинення злочину, який зазначений в диспозиції конкретної кримінально-правової норми.

Характерними рисами кіберзлочинів в Україні є:

1) вчиняються особливими способами і прийомами: за допомогою програмно-технічних засобів, та їх відповідного програмного забезпечення, систем і засобів зв'язку, в тому числі мобільних (в зв'язку з цим підкреслимо, що найбільш поширеним, є

шахрайство з використанням інтернет-банкінгу і мобільних систем зв'язку);

2) протиправні дії відбуваються у віртуальному просторі, зокрема:

– в його глобальних і транскордонних масштабах, при цьому програмно-технічні засоби і сервери, які використовуються зловмисниками, можуть перебувати не в одній державі і до того ж мігрувати, наприклад, в разі поширення нелегального контенту;- географічних рамках двох і більше держав; в національних рамках однієї держави або певної його території.

Відзначимо, що конвергенція і глобалізація кіберзлочинності зростає зі збільшенням кількості і поліпшенням технічних можливостей комп'ютерів, з розвитком їх програмного забезпечення, з вдосконаленням кібернавичок злочинців.

3) вчиняються, як правило, приховано, а не очевидно, тобто вони відносяться до категорії неочевидних злочинів, та мають високий рівень латентності;

4) дії злочинців можуть мати як тривалий, так і одноразовий характер, тривалість DoS-, DDoS-атаки, поширення спаму, створення бот-мережі, робота порнотрекера може тривати від декількох секунд до кількох місяців і років, тобто доки у злочинців є можливість для досягнення поставленої мети;

5) під час вчинення злочину можуть використовуватися один, десятки, сотні і тисячі комп'ютерів, наприклад, якщо в програмне забезпечення комп'ютерів запрограмована і використовується розгалужена бот-мережа;

6) суб'єктом протиправного діяння, як правило, є фахівець в області ІТ-технологій, а співучасниками кіберзлочинів є не тільки хакери-професіонали, а й різного роду шахраї, рекетири, терористи, сутенери, педофіли, торговці людьми, зброєю, боєприпасами, наркотиками;

7) суб'єктивним фактором є умисел злочинця, спрямований, як правило, на незаконне збагачення, отримання матеріальних активів незаконними способами. Разом з тим умисел може бути спрямований і на досягнення різного роду політичних та ідеологічних цілей (наприклад, в ході передвиборчої кампанії).

Окрім вище зазначеного слід підкреслити, що:

– цілі кіберзлочинців досягаються шляхом неправомірного використання інформаційно-комунікаційних технологій (ІКТ), особливо мережі Інтернет, мобільних засобів і систем зв'язку;

– застосування сучасних інформаційно-комунікаційних технологій для вчинення злочину створює специфічні проблеми щодо ідентифікації злочинця, самого факту і географічного місця вчинення злочину, оскільки інформаційно-комунікаційні ресурси які використовуються, можуть розташовуватись в багатьох країнах світу;

– докази, що стосуються даних злочинів, можуть зберігатися і передаватися, як правило, тільки по електронних каналах зв'язку (у зв'язку з цим виникає складність збору і закріплення доказів, проведення процесуальних дій);

– кіберзлочини найчастіше вчиняються для досягнення корисливої мети, проте цілі можуть бути і політичними, і економічними, і терористичними;

– зростає і стає стійкою тенденція до організованості кіберзлочинності, причому об'єднання злочинців відбувається на добровільній основі.

Отже, для вирішення проблеми запобігання кіберзлочинності необхідно перейти до активної розробки ефективної моделі інформаційної безпеки на випередження, та об'єднати зусилля правоохоронних органів, бізнес структур, громадських організацій та IT-корпорацій.

Список використаних джерел

1. Підсумки 2018 року Департамент кіберполіції Національної поліції України Режим доступу: https://cyberpolice.gov.ua/results/2018/

Василевич Віталій Вацлавович,
учений секретар секретаріату Вченої ради Національної академії внутрішніх справ, кандидат юридичних наук, професор;
Пашковська Марина Віталіївна,
старший науковий співробітник наукової лабораторії з проблем превентивної діяльності та запобігання корупції Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ВЗАЄМОДІЯ ПОЛІЦІЇ ТА ГРОМАДИ В ЗАПОБІГАННІ ЗЛОЧИНАМ

Анотація. У тезах досліджуються питання співпраці поліції та громади у запобіганні злочинам та іншим правопорушенням. Розкривається зміст і завдання взаємодії на прикладі реалізації всеукраїнського проекту «Розвиток Community Policing в Україні» розпочатого в м. Києві у травні 2017 року. Обґрунтовується потреба запровадження такого проекту, де поліція разом із громадою формує та підтримує безпечне соціальне середовище.

Розкриваються співпраця громадської організації DreamKyiv (за підтримки Міжнародного фонду «Відродження») і поліції з метою запровадження нового медіапроекту #поліція_відкрита та в рамках реалізації програми «Шкільний офіцер поліції».

З'ясовуються форми взаємодії громадських формувань з охорони громадського порядку і державного кордону, що можуть бути створені