Львівський державний університет внутрішніх справ

ТЕОРІЯ ТА ПРАКТИКА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Міжнародна
науково-практична конференція

11 листопада 2016 року

Львів

УДК 34
ББК 67
Т11

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол від 26 жовтня 2016 р. № 4)

Упорядник – ***Ю. С. Назар***,
кандидат юридичних наук, професор,
директор інституту з підготовки фахівців
для підрозділів Національної поліції
Львівського державного університету внутрішніх справ

Теорія та практика правоохоронної діяльності: Міжнародна
Т11 науково-практична конференція (11 листопада 2016 року) / упор.
Ю. С. Назар. – Львів: ЛьвДУВС, 2016. – 460 с.

Збірник містить тези доповідей учасників Міжнародної науково-практичної конференції «Теорія та практика правоохоронної діяльності», що відбудеться 11 листопада 2016 року у Львівському державному університеті внутрішніх справ.

У наукових розвідках, зокрема, розглянуто питання нормативно-правового забезпечення правоохоронної діяльності; реформування правоохоронної системи; взаємодії правоохоронних органів у правозастосовній діяльності; сучасного стану діяльності правоохоронних органів у сфері протидії злочинності тощо.

Тези опубліковано в авторській редакції.

УДК 34
ББК 67

М. В. Мордвинцев,
кандидат технічних наук, доцент, доцент кафедри
інформаційної безпеки факультету № 4;
В. В. Лейко,
курсант факультету № 4
(Харківський національний університет
внутрішніх справ)

ВЗАЄМОДІЯ ПІДРОЗДІЛІВ ПОЛІЦІЇ З МЕТОЮ ПІДВИЩЕННЯ РОЗКРИТТЯ ЗЛОЧИНІВ

В останні роки, в результаті інтенсивного розвитку інформаційних технологій, з'явились нові види інформаційних продуктів і послуг, які полегшили процес отримання, обробки та використання інформації, передачі її каналами зв'язку в Інтернеті. Виникла необхідність в інформаційній безпеці.

Велика увага сьогодні приділяється нормативно-правовому забезпеченню цієї діяльності. Базові основи закладаються Конституцією України (ст.ст. 17, 19, 31, 32, 34, 50, 57 і 64), Закон України «Про інформацію» регулює правові основи в інформаційній діяльності. Крім цього цілий ряд законодавчих актів регулює відносини в інформаційній сфері. Це, зокрема, Закону України «Про телекомунікації», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», а до Кримінального кодексу України був введений розділ XVI [1], в якому визначалася відповідальність за злочини в інформаційній сфері.

З'явилися нові види злочинів в інформаційній галузі. Це, насамперед, стосується банківської діяльності, де мова йде про обробку транзакцій проведених з грошовими коштами. Тобто в сфері використання платіжних систем.

Такі злочини як скімінг [2] – незаконне копіювання вмісту треків магнітної стрічки (чіпів) банківських карт, кеш-тріппінг – викрадання готівки з банкомату шляхом установки на шатро банкомату спеціальної утримуючої накладки, кардинг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджений її власником, несанк-

ціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

У сфері електронної комерції та господарської діяльності це фішинг – виманювання у користувачів Інтернету їх логінів і паролів до електронних гаманців, сервісів онлайн-аукціонів, переведення або обміну валюти; онлайншахрайство – заволодіння коштами громадян через Інтернет-аукціон, Інтернет-магазин, сайти або телекомунікаційні засоби зв'язку.

У сфері інтелектуальної власності це піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті, кардшаринг – надання незаконного доступу до перегляду супутникового і кабельного ТБ.

У сфері інформаційної безпеки це 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.

Поява такого ряду злочинів викликало створення нового підрозділу правоохоронних органів – кіберполіції. Основні завдання цього органу: реалізація державної політики з протидії кіберзлочинності; протидія кіберзлочинності в сфері використання платіжні систем, електронної комерції та господарської діяльності, інтелектуальної власності та інформаційної безпеки; інформування населення про нові кіберзлочини; впровадження програмних засобів для систематизації і аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини; реагування на запити зарубіжних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів; участь у підвищенні кваліфікації співробітників поліції по застосуванню комп'ютерних технологій у протидії злочинності; участь в міжнародних операціях.

До складу кіберполіції набирають інспекторів і спецагентів. Від одного до чотирьох спецагентів на область України і від шести до чотирнадцяти інспекторів. Передбачається, що чітка взаємодія цих підрозділів може значно підвищити ефективність боротьби з кіберзлочинністю.

Завданням інспектора є видобуток інформації класичними методами оперативно-розшукової діяльності, передбаченої законами України. В його обов'язки входить відкриття кримінальних справ на підставі заяв постраждалих. Далі інспектор через рішення суду домагається, наприклад, відкриття банківської таємниці та отримання доступу до інформації за картковими операціями, телефоном шахрая або доступ до інших ресурсів. Проводить операції, передбачені законом про оперативно-розшукову діяльність, проводить певну аналітичну роботу. Визначає фізичне місцезнаходження особи.

Спецагент надає допомогу інспектору де його технічних знань не достатньо. На підставі інформації, видобутої інспектором, а також інших додаткових даних, здобутих технічними засобами, спецагент допомагає обробляти інформацію з технічної точки зору.

На відміну від звичайних злочинів (вбивство, грабіж, крадіжка), де місце злочину локалізовано, є свідки, очевидний збиток, в кіберзлочини буває багато ситуацій, коли немає свідків, складно зрозуміти, як відбувається злочин.

Для розкриття злочину необхідно аналізувати технічні пристрої і системи, проводити їх технічну експертизу. Таким чином, завдяки роботі спецагентів в технічній галузі складається єдина картина злочину.

Важливим питанням взаємодії інспекторів і спецагентів є транскордонність злочину. Злочинець використовуючи мережу Інтернет може вчиняти злочин одночасно на території декількох країн.

У цьому випадку буде задіяний Національний контактний пункт реагування на кіберзлочини в Україні, який необхідний для обміну інформацією поліцейського характеру між державами.

Спільна взаємодія підрозділів кіберполіції дозволить значно підвищити ефективність боротьби з кіберзлочинцями.

---

1. Кримінальній кодекс України / Стаття 361 – 365.
2. Реалізація державної політики у сфері протидії кіберзлочинності. – Режим доступу: http://www.mvs.gov.ua/ua/