Лисенко Наталія Василівна, слухач навчально-наукового інституту № 4 Національної академії внутрішніх справ
Науковий керівник: кандидат юридичних наук, провідний науковий співробітник відділу організації науково-дослідної роботи Національної академії внутрішніх справ ***Севрук В. Г.***

ЗАХОДИ ПРОТИДІЇ ШАХРАЙСТВАМ, УЧИНЕНИМ ІЗ ВИКОРИСТАННЯМ МЕРЕЖІ ІНТЕРНЕТ

Розвиток та інтенсивне впровадження сучасних інформаційних технологій в різних сферах життєдіяльності обумовлює зростання злочинних проявів в них, що представляє дуже серйозну загрозу як для економіки, так і для інформаційної безпеки держави, складової національної безпеки. Особливо це відчувається з приєднанням до міжнародних систем телекомунікації та підвищення інтелектуального рівня зловмисників, які через мережу Інтернет отримують доступ до комп'ютерної інформації. Високотехнологічні злочини набувають усе більш організованого, транснаціонального характеру [1, с. 106].

Під ризик шахрайських дій потрапляють як державні, так і приватні фінанси. Шахрайство вчиняється як внутрішньо-корпоративними учасниками операцій, так і суб'єктами ззовні. Під удар потрапляють всі сфери суспільних відносин: кредитно-банківська, страхова, мережа Інтернет, зовнішньоекономічна діяльність тощо, що робить означену проблему проблемою транснаціонального характеру [2, с. 230].

Вигідний шахраям і нігілізм українських споживачів у правильному користуванні інтернет-технологіями, онлайн-послуг та недосконаліть відповідного нормативно-правового регулювання

На сьогоднішній день питаннями боротьби із Інтернет-шахрайством в Україні займається Управління боротьби з кіберзлочинністю МВС України. Хоча, слід зазначити, що боротьба зі злочинністю у сфері високотехнологічного шахрайства здійснюється не лише цим підрозділом, а й іншими підрозділами Національної поліції України при тісній взаємодії з підрозділами інших правоохоронних органів.

На нашу думку, основними напрямками протидії Інтернет-шахрайству, на наш погляд, можуть стати:

1) розробка нового програмного обладнання та антивірусних програм;

2) удосконалення нормативно-правової бази у сфері боротьби з Інтернет-шахрайством (жодні технології протидії без відповідної нормативно-правової та методологічної підтримки не зможуть подолати кіберзлочинність).

3) створення системи аутентифікаціїінтернет-адресів для перевірки відповідності введеної користувачем адреси дійсному серверу;

4) підвищення загального рівня грамотності інтернет-користувачів та більш широке поширення інформації про відомі види Інтернет-шахрайства користувачам Інтернету;

5) проведення різного роду науково-практичних конференцій, семінарів, круглих столів за участю теоретиків та практичних працівників.

Так, наприклад, протягом останніх трьох років в Москві було проведено вже 3 міжнародних конференції на тему «Борьба с мошенничеством в сфере високих технологий. Профилактика и противодействие». Наступна конференція запланована на листопад 2013 року, коли пройде 4-та міжнародна конференція по боротьбі із шахрайством у сфері високих технологій «Antifraud Russia – 2013». За роки свого існування конференція зарекомендувала себе як унікальний професійний майданчик для обговорення всього комплексу питань профілактики, запобігання й розслідування шахрайства з використанням комп'ютерних технологій, юридичних аспектів боротьби з кіберзлочинами, притягнення зловмисників до відповідальності [3]);

6) створення в Україні Бази данних інтернет-інцидентів та Центру скарг Інтернет-злочинності за аналогією із IC3 (Internet Crime Complaint Center – США) та RU CERT (Центр реагування на комп'ютерні інциденти Російської Федерації) та ін. [4]).

Окрім зазначеного, необхідно:

1) при здійсненні фінансових операцій в мережі Інтернет, завжди перевіряйте наявність відповідної ліцензії у фінансовій установі та інші дозвільні документи;

2) самостійно здійснюйте моніторинг мережі Інтернет, особливу увагу звертайте на відгуки про підприємство.

Як правило, сумнівні фінансові установи заманюють потенційних клієнтів заниженою відсотковою ставкою;

3) звертайте увагу на назву підприємства, оскільки окремі товариства маскують її під назви відомих банківських та фінансових установ.

4) якщо у Вас виникли певні підозри щодо діяльності таких організацій, терміново повідомте про це до найближчого райуправління поліції [5].

Відповідальність за даний вид злочинів передбачена Кримінальним кодексом України, а саме: ст. 190 «Шахрайство» – карається штрафом або, в залежності від обтяжуючих обставин, позбавленням волі на строк від 5–12 років; ст. 209 КК України «Легалізація (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом» – карається штрафом або, в залежності від обтяжуючих обставин, карається позбавлення волі на строк від 5 до 12 років. Таким чином, на основі вище викладеного можна зробити висновки, що шахрайств що вчиняються в мережі Інтернет є специфічною, адже злочинець підбирає всі можливі засоби, які можна використати в електронному середовищі.

Список використаних джерел

1. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток. Науково-практичний посібник / В.М. Бутузов, В. Д. Гавловський, К. В. Тітуніна, В. П. Шоломенцев; За ред. І. В. Бондаренка. – К., 2009. – 182с.

2. Чернишов Г. М. До питання про визначення фінансового шахрайства / Г. М. Чернишов // Науковий вісник Ужгородського національного університету. Серія: Право. – 2014. – Вип. 26. – С. 230–234.

3. Борьба с мошенничеством в сфере высоких технологий // [Электронный ресурс]. – Режим доступа: http://antifraudrussia.ru/news/339.html.

4. Сабадаш В. П. Інтернет-шахрайство: реалії сучасності та криміналістичні аспекти протидії / В. П. Сабадаш // Ученые записки Таврического национального университета им. В. Вернадского. Серия Юридические науки 2013. – Том 26 (65) – № 1. – С. 278–283.

5. Нечипорук О. Як уберегтися від інтернет-афер [Електронний ресурс]. – Режим доступу : https://kyiv.npu.gov.ua/uk/publish/article/108165.