посилення ролі еколого-правової освіти, удосконалення методики викладання екологічного права та спецкурсів з еколого-правових дисциплін.

Вимоги до впровадження еколого-правової компоненти професійної підготовки практиків природокористування підтверджується змістом Рішення колегії Міністерства освіти і науки України «Про екологізацію вищої освіти України з метою підготовки фахівців для сталого розвитку» від 27.11.2015. Вказаним документом визнано, що екологізація національної освіти на сучасному етапі її реформування – одне з найважливіших стратегічних завдань.

Література

1. Голян В. А. Формування інституціонального механізму екологозбалансованого водокористування / В. А. Голян // Актуальні проблеми економіки. – 2008. – № 9 – С. 145-154.

2. Матвійчук А. В. Екологічна деонтологія: філософсько-методологічне осмислення наукових перспектив: монографія / А. В. Матвійчук. – Рівне: О. Зень, 2014. – 400 с.

3. Синякевич І. Основні постулати екологічної економіки як теоретична основа екологічної політики / І. Синякевич // Економіка України. – 2006. – № 7. – С. 49-54.

4. Сычёв А. А. Экологическая этика как сфера практических действий. Этика и экология: сб. науч. ст. / А. А. Сычёв // НовГУ имени Ярослава Мудрого. – Великий Новгород, 2010. – С. 67-92.

5. Яцик А. В. Екологічна ситуація в Україні і шляхи її поліпшення / А. В. Яцик. – К.: Оріони, 2003. – 84 с.

6. McCormick, John, Environmental Policy in the European Union, Palgrave McMillan, Basingstoke, 2001. – 352 p.

УДК 341:004 (043.2)

Лащенко Є. Д., Широких І. В., студенти,
Навчально-науковий Інститут комп'ютерних
інформаційних технологій,
Національний авіаційний університет, м. Київ
Науковий керівник: Миронець О. М., старший викладач

ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ІНТЕРНЕТ-ШАХРАЙСТВА

У сьогодні Інтернет відіграє дужу важливу роль у житті людства. На жаль, урізноманітнилися способи незаконного заволодіння чужим майном через всесвітню мережу, тому проблема інтернет-шахрайства має актуальний характер.

Поняття вказаного злочину розкриває Кримінальний кодекс України,

відповідно до якого шахрайством вважається заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [1, с. 190].

Шахрайство – поліморфне, тобто може мати декілька форм. Під формою у звичайному слововживанні розуміють спосіб існування змісту, його внутрішню структуру, організацію і зовнішній вираз. Виходячи з вказаного, змістом цього злочину є заволодіння чужим майном, а способом існування його змісту є обман і зловживання довірою. Таким чином, основними формами шахрайства є обман і зловживання довірою [2].

Інтернет-простір уже став частиною нашого реального життя. Нові інтернет-технологій сприяють збільшенню можливостей для скоєння шахрайства, адже потенційними жертвами шахрайства є мільйони користувачів Інтернет-мережі. Але притягнути шахрая до відповідальності законним шляхом складно, у адвокатів, як правило, відсутнє бажання братися за такі справи у зв'язку зі складністю одержання доказової бази. Законодавство України щодо вказаного злочину містить тільки загальні поняття, наприклад: ухилення від сплати податків, розповсюдження реклами, яка є поза законом, порушення прав споживачів, незаконна підприємницька діяльність і т.п., проте вичерпної відповіді щодо видової класифікації інтернет-шахрайства на сьогодні немає.

Одним із напрямів розповсюдження вказаного злочину є соціальні мережі, які активно використовуються великою кількістю як фізичних, так і юридичних осіб практично щодня. Вказаний спосіб комунікації надає багато можливостей для втілення аферистами злочинних намір щодо незаконного заволодіння чужим майном. Велика кількість користувачів та значний рівень довіри серед них до один одного є сприятливим середовищем для вказаного виду шахрайства. Наприклад, за допомогою «спаму», тобто розповсюдження реклами або ж іншої інформації, пропозицій через аккаунт користувача мережі, злочинці, наприклад, впливають на користувачів, а також схиляють до поділу конфіденційною інформацією.

Іншим напрямом шахрайства з використанням новітніх технологій є «фішинг», який полягає у тому, що аферист, використовуючи різні способи, намагається отримати інформацію власника банківської картки. Це може бути підроблений лист, наприклад, від банку або платіжної системи, клієнтом якої є власник картки, із проханням так чи інакше повідомити інформацію, за допомогою якої шахрай може одержати доступ до коштів – запит PIN-коду, логіна, пароля тощо. Найпростіший спосіб «фішингу» – підробка листа. Користувач одержує лист з пропозицією перейти за посиланням, адреса якого схожа на адресу відомої користувачу компанії. Якщо користувач перейде за посиланням та вкаже дані доступу,

які звичайно використовує для доступу до Інтернет-банкінгу або особистого кабінету, його персональні дані стануть доступними шахраям. Крім того, «фішери» активно використовують бот-мережі з метою «витягування» особистих даних користувачів. Така схема дозволяє з кожного наступного зараженого комп'ютера отримати список адрес електронної пошти й використовувати його для розширення бот-мережі з отримання конфіденційної інформації [3]. На нашу думку, Інтернет-користувачам завжди потрібно бути дуже уважними до вказаного характеру листів та за наявності сумнівів телефонувати до банку, де обслуговується клієнт, переконатися в тому, що інформація, запитується саме представником банку.

Найпоширенішим напрямом в інтернет-шахрайстві є різноманітні інтернет-аукціони, інтернет-магазини. У повсякденному житті, коли ми традиційно обираємо потрібний товар в спеціалізованому магазині, шанс стати жертвою шахрайства набагато менший ніж в інтернет-мережі. В Інтернеті наш реальний досвід вибору товарів не приносить ніякої користі – ми позбавлені можливості торкатися, перевіряти працездатність і відсутність вад в об'єкті покупки [4].

На жаль, у наш час високої Інтерент-злочинності бути впевненими у захисті персональних даних досить складно. Інтернет-користувачі з метою превенції вчинення шахрайських дій щодо них можуть, наприклад, убезпечити свою електронну пошту, так як більшість вірусних листів, підозрілих повідомлень приходить саме туди, встановивши надійне антивірусне програмне забезпечення на комп'ютер та зв'язавши його з поштовою скринькою, щоб листи, які мають виконуванні вкладення, перевірялись і у разі небезпеки для користувача автоматично видалялися на поштовому сервері. Користувачам соціальних мереж краще часто змінювати паролі доступу до власної інформації в мережі Інтернет, а також уникати збереження особистих даних на жорсткому диску власного комп'ютера. Варто регулярно встановлювати оновлення для операційної системи комп'ютера, поштового клієнта, антивірусного програмного забезпечення. Дуже дієвим способом захисту від інтернет-шахрайства є використання спеціального модуля firewall, який є комплексним апаратним засобом, пропускає безпечну інформацію та блокує небезпечну через локальну мережу чи Інтернет, тобто повністю контролює інтернет-трафік.

Література

1. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2341-14/page6 стаття 190

2. Мего-Інфо-Юридична бібліотека № 1 [Електронний ресурс]. – Режим доступу: http://mego.info/матеріал-12-види-та-форми-шахрайства#ftn61

3. Абрамов К. Інтернет-шахрайство з платіжними картками та методи захисту від нього / К. Абрамов // Україна фінансова, інформаційно-аналітичний

портал Українського агентства фінансового розвитку [Електронний ресурс]. – Режим доступу: http://ufin.com.ua/analit_mat/poradnyk/094.htm

4. Шахрайство при покупках і продажах в мережі Інтернет. Незалежна асоціація банків України ваш захисник від кіберзлочинності [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/article_detail.php?id=133

УДК 341.824:338.47 (043.2)

Лебедь Н. В., Гришко Н. С., студентки,
Навчально-науковий Інститут комп'ютерних
інформаційних технологій,
Національний авіаційний університет, м. Київ
Науковий керівник: Миронець О. М., старший викладач

ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ПРАВОПОРУШЕННЯ В СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

З розвитком комп'ютерних технологій, які пов'язані зі збереженням, обробкою, передачею інформації, зростає залежність суспільства від роботи комп'ютерної техніки. Практично вся документація юридичних осіб, операції з валютою, відео та фотографії знаходяться у відкритому доступі в режимі онлайн. Звичайно, з одного боку «комп'ютеризація» комунікації між людьми, засобів виробництва дозволяє робити велику кількість необхідних операцій за менші проміжки часу, що значно полегшує життєдіяльність. Проте з іншого боку у наші дні зважаючи на вказане вище створено сприятливі умови для безперешкодного одержання сторонніми людьми, які маючи певні знання комп'ютерної науки, важливої, а головне секретної інформації. Використання вказаних даних звичайно може здійснюватися зі злочинною метою, порушувати права, свободи та законні інтереси людини і громадянина. На сьогодні в Україні кількість злочинів, які вчинено у сфері використання електронно-обчислювальних машин дедалі збільшується, тому питання захисту громадян від правопорушень у комп'ютерній сфері, безперечно, є актуальним.

Поняття правопорушень у сфері комп'ютерної інформації можна з'ясувати досліджуючи поняття комп'ютерної злочинності, яка є особливим видом злочинів, які посягають на встановлений в суспільстві порядок інформаційних відносин та скоюються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Об'єктом злочину виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється