

Хахановський Валерій Георгійович – професор кафедри інформаційних технологій Національної академії внутрішніх справ, доктор юридичних наук

Проблеми боротьби з організованою кіберзлочинністю в економічній сфері

У статті розглядаються теоретичні проблеми боротьби з організованою кіберзлочинністю в економічній сфері, надані практичні рекомендації щодо їх вирішення.

Ключові слова: організована кіберзлочинність, кіберпростір, кібершахрайство, основи національної безпеки України, кібернетична безпека, фішинг; клікджекінг, сайт “Антикібер”.

Останнім часом у світі спостерігається поширення проявів організованої злочинності з використанням глобальної інформаційної мережі Інтернет. Окремим питанням організованої кіберзлочинності присвячено роботи як вітчизняних, так і зарубіжних науковців, зокрема: В. М. Бутузова, В. Б. Вехова, В. Д. Гавловського, В. А. Голубєва, М. В. Гуцалюка, О. Ф. Долженкова, Р. І. Дремлюги, М. Ю. Литвинова, А. А. Небитова, Д. Й. Никифорчука, О. М. Юрченка, С. С. Чернявського, В. П. Шеломенцева та інших.

Разом з тим, у вказаних та інших роботах розглядаються переважно загальні аспекти кіберзлочинності, або певні прояви традиційної організованої злочинності з використанням глобальних інформаційних мереж.

Відомо, що організована злочинність у чинному національному законодавстві (відповідно до Закону України “Про організаційно-правові основи боротьби з організованою злочинністю”) визначається як сукупність злочинів, що вчиняються у зв’язку зі створенням і діяльністю організованих злочинних угруповань [1].

Проте, деякі науковці відзначають, що висока соціальна небезпека кіберзлочинності впливає, насамперед, із суспільних відносин, яким вона загрожує, а також з її транснаціонального та організованого характеру [2, с. 4].

Останнім часом спостерігається стійка тенденція до об’єднання хакерів у групи, які мають чітко виражені ознаки організованих зло-

чинних угруповань [3; 4, с. 113]. Яскравим прикладом прояву організованої злочинності у кіберпросторі можна навести діяльність міжнародного злочинного угруповання під назвою “CarderPlanet” [5; 6].

Ми у цілому підтримуємо позицію В. П. Шеломенцева, який визначає організовану кіберзлочинність як сукупність кіберзлочинів, що вчиняються у зв'язку зі створенням і діяльністю у кіберпросторі організованих злочинних угруповань (кіберугруповань) [7, с. 316].

Разом з тим, сфера боротьби з кіберзлочинністю сьогодні вкрай потребує, у першу чергу, визначення відповідної термінології. Цьому сприятиме прийняття законопроекту про внесення змін до Закону України “Про основи національної безпеки України”, який у 2013 році було зареєстровано Верховною Радою України, і спрямований на формування засад державної політики у сфері забезпечення кібернетичної безпеки нашої держави [8].

Слід зазначити, що Кримінальним кодексом України передбачено відповідальність за вчинення злочинів у сфері дистанційного банківського обслуговування та використання платіжних карток за такими складами:

- крадіжка (ст. 185);
- шахрайство (ст. 190), причому ч. 3 обумовлено вчинення таких дій шляхом незаконних операцій з використанням електронно-обчислювальної техніки;
- незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200). Під документами на переказ розуміються документ у паперовому або електронному виді, що використовується банками чи їх клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів;
- незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231);
- підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів (ст. 358);
- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електров'язку (ст. 361);
- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361¹) [9].

Щодо шахрайства у мережі Інтернет, А. А. Небитов та Л. В. Лефтеров виділяють такі його прояви: отримання зловмисниками як передоплати грошової винагороди за неіснуючий товар; фішинг; клікджекінг тощо. Вказані автори особливо відзначають шахрайство, що вчиняється у сфері дистанційного банківського обслуговування (так

званий Інтернет-банкінг), яке є найважчим видом шахрайства з точки зору його організації, потребує наявності декількох виконавців, а, отже, має ознаки організованого злочинного угруповання [10, с. 53].

За інформацією Національного банку України, поширення безготівкових операцій призводить до зростання кількості випадків шахрайських схем з використанням платіжних карток і несанкціонованого переказу коштів із рахунків клієнтів. Найчастіше злочинці незаконно привласнюють гроші за допомогою підроблених і втрачених платіжних карток, розрахункових операцій без пред'явлення картки (в мережі Інтернет, за допомогою телефону і т. ін.). Українська міжбанківська асоціація членів платіжних систем ЕМА констатує збільшення виявлених торік скімінгових пристроїв на банкоматах і терміналах на 78 % порівняно з 2011 роком. Кількість скімінгових пристроїв у 2012 р. зросла майже вдвічі – з 45 до 80 (поки в Україні рівень цього виду шахрайства є найнижчим у Європі: у 2012 р. один такий пристрій було виявлено на 500 банкоматах, в Україні – у середньому 1,5 пристрою на 10 тис. банкоматів).

За даними НБУ, в загальному обігу за платіжними картками питома вага збитків від шахрайства складає менш ніж 0,002 %. Це небагато, але банки і платіжні системи не показують реальних збитків для збереження довіри клієнтів.

За даними управління боротьби з кіберзлочинністю МВС України, у 2012 р. було зафіксовано 139 фактів несанкціонованого списання коштів з рахунків підприємств із порушенням роботи систем дистанційного банківського обслуговування. Загальна сума збитків склала понад 116 млн грн, з яких 75 % було повернуто. На початку цього року вже зафіксовано 14 таких фактів на загальну суму 9,4 млн грн, з них вдалося повернути потерпілим близько 8,3 млн, тобто 88 %.

Однак повернути гроші реально лише на етапі їх викрадення, тобто тоді, коли кіберкрадіжка лише готується. Вже зняті з банківської картки гроші повертаються власникам досить рідко, оскільки потрібно відшукати злочинця, який діяв через мережу. Крім того, у зловмисника рідко виявляють вкрадені кошти – їх або вже витратили, або “відмили” на різних банківських рахунках.

У 2013 році Незалежна асоціація банків України (НАБУ) в рамках реалізації проекту “Протидія кіберзлочинності” відкрила сайт “Антикібер” (<http://anticyber.com.ua>). Партнерами НАБУ виступають Національний банк України (НБУ), Управління боротьби з кіберзлочинністю МВС України та Національна академія внутрішніх справ.

На сайті збираються дані про види махінацій з банківськими картками і надаються відповідні рекомендації з протидії шахрайству. Новостворений сайт, перш за все, скерований на допомогу користувачам фінпослуг. За допомогою ресурсу можна дізнатися про різні види кібе-

ршахрайств, методи збереження своїх грошей від зазіхань зловмисників і схеми відповідних дій, якщо кошти з рахунку все-ж таки зникли.

Одним із основних напрямів проекту є створення на базі НБУ єдиного інформаційного ресурсу для банків, який дозволить їм обмінюватись та отримувати в оперативному режимі інформацію про нові види й методи кібершахрайства для своєчасного вживання попередніх заходів.

Загалом правоохоронці очікують від реалізації проекту “Протидія кіберзлочинності” не лише підвищення ефективності взаємодії, але й реалізації елементарних заходів профілактики, до яких може вдатися кожен українець, щоб захистити свою власність. Найперше, що варто зробити, – це відповідально ставитися до власних персональних даних.

Отже, враховуючи викладене вище, можна констатувати, що вжиття низки заходів організаційного та нормативно-правового характеру, зокрема розвиток новоствореного сайту “Антикібер”, та прийняття Верховною Радою України у найближчий час законопроекту про внесення змін до Закону України “Про основи національної безпеки України” дозволить підвищити рівень боротьби з організованою кіберзлочинністю в сфері економіки.

Список використаних джерел

1. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30 черв. 1993 р. № 3341-ХП // Відомості Верховної Ради України. – 1993. – № 35. – Ст. 358.

2. Дремлюга Р. И. Интернет-преступность : автореф. дис. на соискание ученой степени канд. юрид. наук : спец. 12.00.08 “Уголовное право и криминология; Уголовно-исполнительное право” / Р. И. Дремлюга. – Владивосток, 2007. – 26 с.

3. Кузнецов А. Борьба с преступлениями, совершаемыми с использованием сети Интернет [Электронный ресурс] / Антон Кузнецов. – Режим доступа : <http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=593>.

4. Долженков О. Ф. Инфраструктура організованої економічної злочинності / О. Ф. Долженков. – Одеса : НДРВВ ОЮІ НУВС, 2002. – 254 с.

5. Хвостик Е. Украинских карточных мошенников вытянули из сети / Е. Хвостик, Е. Ковалева, М. Никитин // Коммерсантъ. – 2005. – № 132 (3216). – 20 июля.

6. Золотое время Carderplanet / [Электронный ресурс]. – Режим доступа : <http://www.interface.ru/home.asp?artId=2217>.

7. Шеломенцев В. П. Организована кіберзлочинність: до визначення поняття / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 21. – С. 314–322.

8. Про внесення змін до Закону України “Про основи національної безпеки України” щодо кібернетичної безпеки України : законопроект від 7 берез. 2013 р. / [Електронний ресурс]. – Режим доступу : <http://wl.cl.rada.gov.ua/pls/zweb2/webproc4>.

9. Кримінальний кодекс України // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.

10. Небитов А. А. Шахрайство у сфері електронної комерції / А. А. Небитов, Л. В. Лефтеров // Боротьба з Інтернет-злочинністю : матеріали міжн. наук.-практ. конф. (м. Донецьк, 12–13 черв. 2013 р.). – Донецьк : ДЮІ МВС України, 2013. – С. 52–55.

В статье рассматриваются теоретические проблемы борьбы с организованной киберпреступностью в экономической сфере, даны практические рекомендации по их решению.

The article discusses the theoretical problems of combating organized cybercrime in the economic sphere; the practical recommendations to debate them are given.

Стаття надійшла до редакції журналу 29 липня 2013 року.