УДК 343.537

О.Б. Сахарова,
кандидат юридичних наук,
старший науковий співробітник

ОСОБЛИВОСТІ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СИСТЕМІ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ

У статті розглядаються деякі особливості вчинення кримінальних правопорушень у системі дистанційного банківського обслуговування (далі – ДБО). Автор намагається висвітлити чинники, що є передумовою вчинення правопорушень у сфері функціонування ДБО, та узагальнити ознаки, які можуть використовуватися оперативними працівниками органів внутрішніх справ для виявлення вчинених кримінальних правопорушень з використанням системи дистанційного банківського обслуговування.

***Ключові слова**: дистанційне банківське обслуговування, системи "Клієнт-Банк", "Інтернет-Клієнт-Банк", Інтернет-банкінг, система SWIFT, лог-файли, веб-ресурси, бот-мережі, спам, DoS-атаки, IP-адреса, транзакції, кіберзагрози, кібершпіонаж, кіберзлочинці, Інтернет-шахрайство.*

В статье рассматриваются некоторые особенности совершения уголовных преступлений в системе дистанционного банковского обслуживания (далее – ДБО). Автор пытается осветить факторы, являющиеся предпосылкой совершения правонарушений в сфере функционирования ДБО, и обобщить признаки, которые могут использоваться оперативными работниками органов внутренних дел для выявления совершенных уголовных преступлений с использованием системы дистанционного банковского обслуживания.

***Ключевые слова**: дистанционное банковское обслуживание, системы "Клиент-Банк", "Интернет-Клиент-Банк", Интернет-банкинг, система SWIFT, лог-файлы, веб-ресурсы, бот-сети, спам, DoS-атаки, IP-адрес, транзакции, киберугрозы, кибершпионаж, киберпреступники, Интернет-мошенничество.*

Paper reviews some of the features of criminal offenses in remote banking service (RBS). The author tries to highlight the factors that are the prerequisites for offenses in the functioning of RBS, and to summarize the features that can be used by operative police officers to identify criminal offenses committed with the use of remote banking service.

***Keywords:** remote banking service, "Client-Bank" and "Internet-Client-Bank" systems, Internet banking, SWIFT system, log files, web resources, botnets, spam, DoS-attacks, IP address , transactions, cyber threats, cyber espionage, cyber criminals, Internet fraud.*

За умов суспільної нестабільності та економічного занепаду, посилення структурних деформацій, на фоні послаблення реального впливу держави на економіку та, зокрема, на фінансову систему, як наслідок, відбувається значне зростання кількості корисливих кримінальних правопорушень. При цьому останнім часом у банківських установах акцент зловживань за своїм змістом все помітніше переміщується від правопорушень, пов'язаних з кредитуванням, до вчинення

кримінальних правопорушень у сфері дистанційного банківського обслуговування.

Кримінальні правопорушення у сфері діяльності банківських установ відрізняються значною різноманітністю, особливою витонченістю, високоінтелектуальним характером, активною адаптацією злочинців до нових форм і методів підприємницької діяльності, застосовуванням банківських документів, нових електронних платіжних засобів, засобів зв'язку, а також новітніх банківських технологій щодо забезпечення господарської діяльності.

Особливості вчинення кримінальних правопорушень у сфері кредитно-фінансової та банківської діяльності та проблематика розкриття особливостей та способів їх вчинення вивчалися такими науковцями, як Г. Матусовський, О. Бущан, Д. Березін, А. Волобуєв, О. Волохова, В. Гаєнко, Д. Голосніченко, О. Джужа, В. Лавров, В. Ларичев, Т. Пазинич, В. Попович, Г. Спірін, С. Шаров, С. Чернявський та ін. Виходячи з результатів досліджень цих вчених і досвіду роботи правоохоронних органів, можна стверджувати, що кримінальними правопорушеннями уражені майже всі банківські операції. Проте однією з найбільш вразливих ділянок роботи банківських установ вже багато років залишається ДБО через мережу банкоматів, терміналів самообслуговування та спеціалізованих сайтів. Поряд з цим, зазначені науковці не присвячували достатньої уваги розгляду особливостей вчинення кримінальних правопорушень у системі дистанційного банківського обслуговування. Отже, на підставі аналізу матеріалів практики та наявних наукових праць, присвячених цій проблематиці, ми в статті ставимо за мету визначити характерні особливості вчинення кримінальних правопорушень у системі дистанційного банківського обслуговування з метою подальшої розробки методики ефективного та своєчасного виявлення цих злочинних діянь.

Слід наголосити, що значні обсяги фінансових операцій з використанням банківських систем віддаленого обслуговування клієнтів є основним чинником, який привертає до цієї сфери особливу увагу злочинців. Дії злочинців спрямовані головним чином на отримання надприбутків, що відповідно призводить до збільшення кількості правопорушень саме в банківській сфері діяльності.

За даними Національного банку України, найбільш розповсюдженими в банківських установах видами шахрайства в системах дистанційного банківського обслуговування (ДБО) (системах "Клієнт-Банк" (on-line/off-line), "Інтернет-Клієнт-Банк", Інтернет-банкінг) є такі кримінальні правопорушення [1, с. 10–11]:

• створення комп'ютерних вірусів та троянських програм для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням ДБО;

• відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті несанкціонованих операцій у системах ДБО;

• отримання платежів від закордонних відправників через міжнародну систему SWIFT внаслідок втручання в роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ.

Як відомо, дистанційне банківське обслуговування – загальний термін для технологій надання банківських послуг на підставі розпоряджень, переданих клієнтом віддалено (без візиту до банку). Завдяки системі ДБО клієнти банку готують та направляють у банк на виконання платіжні та інші документи, контролюють стан своїх рахунків. Зв'язок та обмін інформацією між банком та клієнтами в системі "Клієнт-Банк" здійснюється через стандартні комутовані (телефонні) канали зв'язку за допомогою модему. Система "Клієнт-Банк" забезпечує клієнтові

можливість оперативно управляти власними рахунками в банку, не покидаючи свій будинок або офіс.

Користувачів системи "Клієнт-Банк" умовно поділяють на дві категорії. Перша – регіональні підприємства, які не мають можливості постійно їздити в банк, хоча б тому, що вони територіально віддалені від нього. Друга – підприємства, які розташовані у великих містах, але здійснюють дуже багато оперативних платежів.

У процесі вчинення шахрайства в системі дистанційного банківського обслуговування ("Клієнт-Банк", "Інтернет-Клієнт-Банк", системі Інтернет-банкінгу) злочинцями "запускається" вірус типу back-door на комп'ютері жертви (клієнта банківської установи), підключеному до банківської системи "Клієнт-Банк", та здійснюється несанкціонована транзакція нібито від імені цього клієнта. Учасників злочинного угруповання щонайменше троє: хакер – розробляє шкідливу програму і запускає її; "фінансист" – створює систему переказу коштів; третій (фіктивна фірма або фізична особа) – отримує готівку.

Як правило, у проміжок часу між зараженням комп'ютерів та проведенням несанкціонованої транзакції протягом декількох тижнів злочинці відстежують стан рахунків та аналізують технічні особливості з'єднання комп'ютерів клієнтів з серверами банків (лог-файли).

У роботу систем ДБО злочинці найчастіше втручаються шляхом зараження комп'ютера вірусним програмним забезпеченням через шкідливу спам-розсилку, відвідування заражених сайтів або використання заражених флеш-носіїв.

Завантаження вірусу на комп'ютер жертви відбувається практично непомітно. Основне завдання вірусу на початковому етапі – це спостереження, збір інформації і передача його на комп'ютер шахраїв. Вірус може викрадати паролі доступу до систем ДБО, ключі електронного цифрового підпису, зчитувати реквізити платежів. Це також можуть бути програми, що відстежують появу на екрані вікна підключення до ДБО з метою подальшого перехоплення таємної інформації, яка вводиться в це вікно, або копіюють вміст буфера обміну в момент підключення до систем електронних платежів [1, с. 15–16].

Мета шахраїв – спотворити інформацію, сформувати за допомогою ДБО і провести платіж (через підроблені платіжні документи (платіжні доручення) на переказ коштів), який за змістом не буде виділятися в потоці звичайної діяльності жертви, але переведе гроші на рахунки підставної особи або фіктивної фірми, використовуючи звичайне для даного клієнта призначення платежу. Надалі найчастіше кошти, вкрадені з рахунку, переводяться в готівку. Зняття готівки проводиться в основному через банкомати з метою уникнення спілкування з працівниками банку [1, с. 16].

Слід зазначити, що останнім часом все частіше відбувається ураження шкідливими програмами комп'ютерів керівників / головних бухгалтерів підприємств шляхом надсилання зловмисником на електронну пошту жертви (бухгалтера або керівника) листа, який складається таким чином, щоб отримувач без вагань відкрив його (тобто, застосовуються методи соціальної інженерії), а також містить або посилання на шкідливу програму, або додаток зі шкідливою програмою.

Шкідливий файл при його завантаженні начебто виглядає як документ MS Word або архів WinRAR, але має розширення (".exe", ".bin", ".bat", ".dll", ".com", ".sys", ".scr" та ін.; наведений список не є вичерпним).

Реалізації злочинного наміру зловмисника сприяє те, що керівники / відповідальні співробітники підприємств:

• використовують неліцензійне програмне забезпечення (як операційні системи, так і, наприклад офісні програми);

• не перевіряють джерела надходження інформації (приміром, шляхом дзвінка відправнику та перевірки факту відправки ним електронного листа);

• не коректно використовують носії ключової інформації (наприклад, замість підключення USB-токена тільки для здійснення транзакції, підключають його до комп'ютера на весь робочий день);

• застосовують комп'ютери, на яких встановлена система "Клієнт-Банк", для ігор, доступу до Інтернету, перегляду новин, користування соціальними мережами тощо (натомість такий комп'ютер має бути ізольованою автоматизованою системою).

Виділяють такі чинники, що є передумовою вчинення правопорушень у сфері функціонування ДБО, а саме:

• недотримання суб'єктами підприємницької діяльності, державними установами вимог законодавства щодо нерозповсюдження конфіденційних даних (авторизаційних даних користувачів Інтернет-банкінгу, паролів доступу електронних засобів захисту), доступ сторонніх осіб до конфіденційної інформації підприємства, організації. Наприклад, майже завжди серед наявної інформації на персональному комп'ютері користувача зберігаються авторизаційні дані для підключення до системи Інтернет-банкінгу, пароль доступу, за яким виконується транзакція користувачем або підписується документ;

• недостатній захист комп'ютерно-технічних засобів, що працюють у системах ДБО, від зовнішнього Інтернет-середовища, локальної мережі установи, що дає можливість злочинцям отримувати контроль над інформацією та з'єднаннями на веб-ресурсах банків, маніпулювати апаратними можливостями комп'ютерно-технічних засобів з метою об'єднання їх у бот-мережі для розповсюдження спаму чи організації DoS-атак (атак типу "відмова в обслуговуванні", від англ. Denial of Service)). Так, у деяких випадках з аналізу журналів операційної системи, програм захисту, наявності вірусних і троянських кодів, програм та їх залишків стає зрозумілим, що передумовою стороннього втручання (наприклад, транзакції, виконаної з авторизаційними даними від імені іншої особи) є те, що злочинці вивчають час і технічні можливості роботи потенційної жертви на комп'ютері; блокують роботу в мережі та "заражають" інформацію користувача з метою отримання дистанційного контролю над певними технологічними процесами. Сам користувач, а це, як правило, співробітник бухгалтерії підприємства, не в змозі оцінити такі чинники, як: несподівані затримки в роботі комп'ютера та телекомунікаційних засобів, чи завантажена при підключенні веб-сторінка саме ресурсу банківської установи, а не підробка для отримання авторизаційних даних і ключів;

• використання суб'єктами підприємницької діяльності, державними установами неліцензійного програмного забезпечення (особливо операційних систем, програм захисту інформації), внутрішнє ураження вірусами інформації комп'ютера (комп'ютерної мережі) відповідними діями користувача (користувачів).

Індикаторами підозрілості фінансових операцій з точки зору вчинення можливих кримінальних правопорушень у банківських установах, пов'язаних з ДБО, опосередковано можуть бути такі фактори:

• спроба входу із забороненої/нової IP-адреси;

• спроба використання прострочених первинних/робочих або старих ключів після сертифікації нових;

• використання для банківських операцій IP-адрес та імен користувачів, за якими попередній моніторинг виявив причетність до шахрайських операцій;

• транзакції в нестандартний час або підключення до системи у вечірній час;

• незвичайні умови або складність операції: висока частота переказів коштів протягом невеликого періоду часу, велика кількість різноманітних джерел походження коштів та платіжних методів (інструментів);

• особа не інформована про характер діяльності юридичної особи, яку вона представляє;

• особа не може пояснити необхідність надання тієї або іншої банківської послуги;

• залучення до проведення операцій осіб молодого віку та/або новостворених підприємств;

• проведення операцій за втраченими документами;

• відкриття рахунку, на який зараховуються кошти внаслідок несанкціонованого списання, незадовго до проведення таких операцій;

• спроби зняти кошти в день їх зарахування;

• намагання клієнта отримати дві або більше банківських карток, що не відповідає суті його діяльності або обороту;

• зарахування коштів на карткові рахунки фізичних осіб з подальшим зняттям через банкомати (в т.ч. інших банків);

• операції не відповідають попереднім операціям клієнта;

• відсутність інформації щодо господарської діяльності клієнта або використання онлайнових платіжних систем замість традиційних;

• міжнародні перекази, які отримуються/перераховуються з/за кордон, що не відповідає діяльності клієнта.

Основними ознаками (критеріями), які можуть використовуватись оперативними працівниками ДСБЕЗ для виявлення вчинених кримінальних правопорушень з використанням системи дистанційного банківського обслуговування, є [3]:

1) відмінне від справжньої діяльності, сумнівне призначення платежу;

2) проведення операцій у великій кількості за короткий проміжок часу з використанням спеціальних платіжних засобів у мережі Інтернет та точках продажу;

3) повідомлення про введення великої кількості невірних ПІН-кодів при використанні платіжних карт з одного банкомату або точки продажу;

4) клієнт скористався (намагався скористатись) своєю платіжною карткою протягом невеликого проміжку часу з різних місць, які фізично неможливо подолати за цей час;

5) перерахування коштів на суму, що дорівнює або перевищує визначену суму в гривнях або еквівалент цієї суми в іноземній валюті, за допомогою систем дистанційного доступу та управління рахунками через мережу Інтернет з рахунків юридичних осіб − клієнтів банку на рахунки фізичних осіб та карткові рахунки суб'єктів господарювання в інші банки;

6) перерахування коштів, що перевищує визначену суму, з рахунків клієнтів банку, здійснені за допомогою системи Інтернет-банкінг, новому контрагенту на новий рахунок, перерахування коштів з поточного рахунку юридичної особи на рахунок іншої юридичної особи − клієнта іншого банку з призначенням платежу "поповнення поточного рахунку";

7) ЄДРПОУ платника не дорівнює ЄДРПОУ отримувача, МФО банку отримувача не дорівнює МФО банку платника;

8) перерахування коштів, здійснені за допомогою системи Інтернет-банкінгу, з призначенням платежу "фінансова допомога", "повернення фінансової допомоги", "оплата по договору комісії", "повернення/одержання позики", на визначену суму;

9) вимога клієнта видати кошти готівкою, терміново, протягом декількох годин після їх зарахування на рахунок;

10) платіж явно не відповідає напрямку господарської діяльності клієнта банка;

11) платіж містить окремі недоліки в призначенні платежу (відсутнє посилання на утримання податку, наявність ПДВ тощо);

12) код ЄДРПОУ клієнта-отримувача та банка-отримувача співпадає;

13) платіж надійшов в значній сумі, яка є незвичною для клієнта-платника або дорівнює (близька) до залишку на його рахунку.

5 лютого 2013 р. правоохоронці та банкіри підписали Меморандум про співпрацю, що надає можливість банкам в оперативному режимі обмінюватися інформацією про нові види шахрайств, про шкідливі віруси та пристрої для викрадення конфіденційної інформації [4].

Крім того, Українською міжбанківською Асоціацією членів платіжних систем ЄМА та Державним центром захисту інформаційно-телекомунікаційних систем (ДЦЗ ІТС) Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку), на базі якого функціонує CERT-UA (спеціалізований структурний підрозділ ДЦЗ ІТС Держспецзв'язку), у вересні 2014 р. було підписано Меморандум про співпрацю у сфері протидії шахрайству та викраденню грошових коштів з рахунків у банках фізичних та юридичних осіб України, організованого з використанням банківських троянських програм у системі ДБО.

Серед **основних видів кіберзагроз, протидіяти яким доводиться CERT-UA**, можна виділити такі: шкідливе програмне забезпечення (блокування інформації, виведення АС і/або ІС з ладу, кібершпіонаж, несанкціоноване переведення грошових коштів тощо); бот-мережі; Інтернет-шахрайство (фішинг, вішинг тощо); DDoS-атаки; експлуатація вразливостей в програмному і апаратному забезпеченні; несанкціонований доступ до автоматизованих/інформаційних систем, веб-ресурсів та порушення штатного режиму їх функціонування.

Зокрема, фахівцями команди реагування на комп'ютерні надзвичайні події України CERT-UA протягом першого кварталу 2014 р. були зафіксовані численні випадки розсилання електронних листів начебто від імені державних органів України (Міндоходів, Державної реєстраційної служби, НАК "Нафтогаз України" та ін.) [5]. Зазвичай, як додаток до цього електронного листа надсилався файл MS Word, що містив програмний код "всередині" для атаки на обчислювальну систему (CVE-2010-3333, CVE-2012-0158). Під час відкриття файлу відбувалася експлуатація вразливості в програмному забезпеченні MS Word (якщо встановлена версія не була оновленою), а комп'ютер уражався шкідливою програмою (банківським трояном). Як було з'ясовано пізніше, всі уражені в подібний спосіб комп'ютери автоматично "долучалися" до складу бот-мережі, призначенням якої було організація викрадення грошових коштів з систем дистанційного банківського обслуговування за посередництва шкідливої програми.

За період з січня по квітень 2014 р. ідентифікована бот-мережа налічувала 46234 уражених шкідливими програмами комп'ютерів (ботів), а в базі даних серверу управління бот-мережею було близько 40 000 000 одиниць скомпрометованих даних (сертифікат, логін/пароль, зображення з екрану). Також було з'ясовано, що здебільшого жертвами цього кримінального правопорушення були бухгалтери/керівники українських підприємств.

Слід зазначити, що позитивним моментом у протидії кіберзлочинності є запуск сайту "Антикібер", який надає практичні поради про те, як не стати жертвою кіберзлочинців. Реалізація цього сайту дозволяє банкам в оперативному режимі

обмінюватись інформацією про нові види шахрайства, про шкідливі віруси та пристрої для викрадення конфіденційної інформації.

Підсумовуючи, наголосимо, що розглянуті нами особливості та способи вчинення кримінальних правопорушень у системах дистанційного банківського обслуговування не є вичерпними. Водночас розгляд зазначеної вище проблематики дає можливість розробки методик їх виявлення, розкриття та запобігання.

Виявлення та нейтралізація протиправних посягань, що вчиняються у сфері банківської діяльності в системі ДБО, вимагають комплексного підходу та є першочерговим напрямком діяльності як державних правоохоронних органів, так і самих банківських структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кіберзлочинність та відмивання коштів // Департамент фінансових розслідувань Державної служби фінансового моніторингу України. – 2013. – 53 с.

2. Лист Незалежної асоціації банків України до НБУ від 02.09.2013 “Щодо надання інформації з типологічних схем легалізації (відмивання) доходів, пов‘язаних зі злочинами у сфері кіберзлочинності”.

3. Правоохоронці та банкіри підписали Меморандум про співпрацю (прес-служба МВС України) [Електронний ресурс]. – Режим доступу : http : // www.kmu.gov.ua/control/uk/publish/article?art_id=246030781.

4. CERT-UA та ЄМА. Протидія шахрайству в системах ДБО [Електронний ресурс]. – Режим доступу : http : // ema.com.ua/cert_ua_and_ema_fraud_prevention_systems_rbs/.

Отримано 15.09.2015