НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
СЕВАСТОПОЛЬСЬКИЙ ІНСТИТУТ БАНКІВСЬКОЇ СПРАВИ
УКРАЇНСЬКОЇ АКАДЕМІЇ БАНКІВСЬКОЇ СПРАВИ
НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ПРОТИДІЯ ЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ МЕРЕЖ

Тези доповідей Міжнародної
науково-практичної конференції
(Севастополь, 1–2 жовтня 2010 року)

Суми
ДВНЗ "УАБС НБУ"
2010

УДК 343.346.8:004.056.53](043.2)
П83

П83 **Протидія** злочинам, які вчиняються з використанням комп'ютерних мереж [Текст] : тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад "Українська академія банківської справи Національного банку України". – Суми : ДВНЗ "УАБС НБУ", 2010. – 208 с.

Видання містить тези доповідей учасників Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 р.).

Розраховане на фахівців у сфері комп'ютерних технологій, правоохоронних органів, представників банківської системи, науково-дослідних установ і вищих навчальних закладів.

УДК 343.346.8:004.056.53](043.2)

Матеріали збірника подаються в авторській редакції.

ЗМІСТ

Секція 2
МЕТОДОЛОГІЯ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ КОМП’ЮТЕРІВ, СИСТЕМ І КОМП’ЮТЕРНИХ МЕРЕЖ

Секція 3
ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ ТА ВІДМИВАННЮ ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ ЗА ДОПОМОГОЮ ФІНАНСОВИХ ІНСТРУМЕНТІВ, КОМП'ЮТЕРНИХ МЕРЕЖ, БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМ

ВСТУПНЕ СЛОВО!

Шановні учасники конференції! Щиро вітаємо вас з початком Міжнародної науково-практичної конференції "Протидія злочинам, які вчиняються з використанням комп'ютерних мереж".

Характерною рисою сучасного етапу становлення людської цивілізації є надзвичайно високий рівень розвитку інформаційних технологій, які все активніше пронизують усі сфери суспільного життя. Сьогодні жодна галузь вітчизняної чи світової економіки не може існувати без надійних комп'ютерних технологій, тобто технічних ресурсів, програмного забезпечення та систем комп'ютерних мереж. І якщо банківський сектор справедливо називають кровоносною системою економіки, то комп'ютерні мережі та технології можна порівняти з нервовою системою, від надійності та точності функціонування якої залежить не лише взаємозв'язок між різними елементами економічної системи, а й її цілісність і життєздатність загалом.

На жаль, доводиться констатувати, що за нинішнього рівня глобалізації економіки будь-яке санкціоноване чи несанкціоноване втручання в діяльність комп'ютерних мереж у фінансово-банківській сфері, транспорті чи навігації або навіть простий збій у їх роботі може призвести до багатомільйонних втрат і поставити під загрозу життя та здоров'я багатьох тисяч людей. Також не рідкісними є випадки, коли комп'ютерні технології та мережі цілеспрямовано використовуються з метою вчинення різноманітних злочинів – починаючи з порушення авторських прав на комп'ютерні програми та розголошення конфіденційної інформації та закінчуючи викраденням коштів з банківських рахунків і легалізацією коштів, одержаних злочинним шляхом.

Саме тому особливої актуальності набувають питання протидії злочинам, пов'язаним з використанням комп'ютерних мереж. Проблема протидії кіберзлочинам має багатовекторний характер і може вирішуватися лише на основі поєднання комплексу технічних, економічних, організаційних і правових заходів, що мають здійснюватися одночасно на регіональному, національному та міжнародному рівнях.

Сьогодні на базі Севастопольського інституту банківської справи Української академії банківської справи Національного банку України зібралися представники банківської системи та правоохоронних органів, науково-дослідних установ і вищих навчальних закладів. Ця конференція, що проводиться під егідою Національного банку України та Міністерства внутрішніх справ України, стала своєрідним форумом фахівців різного профілю, науковців та практиків, які зібралися з метою обговорення існуючих проблем у галузі боротьби зі злочинами, пов'язаними з використанням комп'ютерних мереж, поділитися власним досвідом у цій сфері та спільно розробити рекомендації щодо підвищення рівня ефективності боротьби з кіберзлочинністю та посилення інформаційної безпеки вітчизняної банківської системи.

Ефективна боротьба зі злочинами, пов’язаними з використанням комп’ютерних мереж, можлива лише за умови тісного співробітництва між банківськими установами, правоохоронними органами, науковими установами та широкими колами громадськості. У межах нашої конференції маємо чудову нагоду для конструктивного діалогу між представниками наукових кіл, органів державної влади та банківської системи, а також обміну ідеями між фахівцями у сфері права, економіки та комп’ютерних систем, які створять міцне підґрунтя для ефективної боротьби з комп’ютерною злочинністю. Тож щиро запрошую вас до участі в роботі конференції!

А.О. Єпіфанов,
д-р екон. наук, проф., ректор
Державного вищого навчального закладу
“Українська академія банківської справи
Національного банку України”

Секція 1

УПРАВЛІННЯ БЕЗПЕКОЮ БАНКУ: ПОЛІТИКА БЕЗПЕКИ, АНАЛІЗ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

Р.В. Кармазин, *начальник відділу Юридичного департаменту Національного банку України*

РЕГУЛЮВАННЯ В УКРАЇНІ ДІЯЛЬНОСТІ З ПРИЙМАННЯ КОШТІВ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ САМООБСЛУГОВУВАННЯ ТА НАПРЯМИ ПРОТИДІЇ ЗЛОЧИННИМ ПРОЯВАМ

Питання поширення комп'ютерної злочинності в Україні та її масштаби здаються багатьом неактуальними. Проте, якщо суспільство адекватно не реагуватиме на такі злочинні прояви, то перед ним постануть значні загрози для його життєдіяльності. Передумовами зростання злочинності у сфері комп'ютерних мереж та високих інформаційних технологій є ускладнення технічних систем зв'язку, спрощення доступу до використання комп'ютерних технологій широкого кола фізичних осіб, підвищення знань осіб, що намагаються вчинити протиправні діяння тощо. Проблемами, які постають у сфері інформаційних та платіжних технологій є те, що злочини, пов'язані з використанням цих високих технологій, виходять за межі звичайних дій в уявлені пересічного громадянина, і представляють собою дії, які станом на сьогодні неврегульовані законодавством повністю або частково. Як зазначають П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. поширення інформаційних технологій має і свій негативний аспект: це відкриває шлях до антисоціальної та злочинної поведінки [1, 57].

Особливої гостроти набуває питання захисту інформації в банківській системі, оскільки по-суті, йдеться про захист власності у вигляді коштів, що залучені банками та небанківськими фінансовими установами.

Відповідно до статті 99 Конституції України [2], основною функцією Національного банку України (далі – НБУ) є забезпечення стабільності грошової одиниці – гривні. Виконання зазначеної функції в частині здійснення контролю за переказами коштів виконується НБУ шляхом застосування статті 40 Закону України "Про Національний

банк України" [3] та статей 41, 42 Закону України "Про платіжні системи та переказ коштів в Україні" [4] щодо здійснення регулювання розрахунків та контролю за діяльністю платіжних систем, дотримання порядку проведення переказів.

Технічний прогрес, потреби ринку та розвиток нових платіжних технологій вивели на ринок платіжні пристрої, що забезпечують застосування спеціальних платіжних засобів та готівки – банкомати, термінали, комп'ютери та програмно-технічні комплекси самообслуговування (далі – ПТКС). Такий вид платіжних пристроїв як ПТКС набув великої популярності у населення, адже це зручний спосіб сплати послуг мобільних операторів, підприємств житлово-комунальної сфери, а також кредитів тощо.

З огляду на поширення здійснення дрібних платежів із застосування ПТКС на користь третіх осіб, що надають послуги ініціаторам переказів, постановою Правління НБУ від 05.03.2008 № 53 "Про врегулювання питань здійснення операцій із застосуванням програмно-технічних комплексів самообслуговування" [5] (далі – Постанова № 53) врегулював, що операції з приймання готівки для подальшого переказу та інші операції, пов'язані з рухом коштів, а також отримання інформації щодо стану рахунків із застосуванням ПТКС, до яких згідно з їх функціональними можливостями належать банківські автомати самообслуговування, депозитні банкомати, платіжні термінали, термінали самообслуговування тощо, можуть здійснювати банки і небанківські фінансові установи, які відповідно до законодавства України отримали відповідну ліцензію/дозвіл щодо переказу коштів органів державної влади, що здійснюють державне регулювання відповідних ринків фінансових послуг, і є платіжними організаціями та/або членами платіжної системи та суб'єкти господарювання, які уклали агентські договори з банками.

Проте зміст діяльності щодо прийому коштів в готівковій формі із застосуванням ПТКС на користь надавачів послуг та його нормативно-правове врегулювання потребує детального наукового вивчення та обґрунтування.

Відповідно до статті 1 Закону України "Про фінансові послуги та державне регулювання ринків фінансових послуг" [6] до фінансових послуг віднесено операції з фінансовими активами, зокрема, коштами, що здійснюються в інтересах третіх осіб за власний рахунок чи рахунок цих осіб. Переказ грошей, відповідно до статті 4 Закону України "Про фінансові послуги та державне регулювання ринків фінансових послуг" [6], є фінансовою послугою.

Стаття 10 Закону України "Про платіжні системи та переказ коштів в Україні" [4] встановлює, що небанківські фінансові установи можуть

здійснювати переказ коштів за допомогою внутрішньодержавних небанківських платіжних систем члени яких, які не є банками, повинні мати ліцензію Державної комісії з регулювання фінансових послуг України (далі – Держфінпослуг) на переказ коштів після реєстрації та отримання дозволу НБУ. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем, затверджене постановою Правління НБУ від 25.09.2007 № 348 [7] встановлює порядок реєстрації та отримання дозволу на діяльність внутрішньодержавної небанківської платіжної системи. Попередньо, для отримання права здійснювати переказ коштів через внутрішньодержавну небанківську платіжну систему юридична особа має, відповідно до статті 7 Закону України "Про фінансові послуги та державне регулювання ринків фінансових послуг" [6], набути статусу фінансової установи. Далі, відповідно до статті 10 Закону України "Про платіжні системи та переказ коштів в Україні" [4], статті 4 Закону України "Про фінансові послуги та державне регулювання ринків фінансових послуг" [6], Ліцензійних умов здійснення переказу коштів небанківськими фінансовими установами, затвердженими Розпорядженням Держфінпослуг від 23.03.2006 № 5523 [8] така фінансова установа має отримати ліцензію на здійснення нею переказу коштів (грошей).

Виходячи із вищевикладеного можна дійти висновку, що прийом коштів у готівковій формі та їх переказ на рахунки третіх осіб (надавачів послуг, посередників тощо), крім банків, мають право здійснювати юридичні особи, що є фінансовими установами, отримали ліцензію Держфінпослуг на переказ коштів та отримали дозвіл НБУ на діяльність внутрішньодержавної небанківської платіжної системи.

Одночасно слід зазначити, що згідно Постанови № 53 [5] право здійснювати діяльність з приймання готівки для подальшого переказу із застосуванням ПТКС надано іншому виду осіб – агентам банків.

Стаття 47 Закону України "Про банки і банківську діяльність" [9], не відносить приймання платежів без застосування рахунків до переліку виключно банківських операцій. Поняття "банківська операція" є одним із основоположних у банківському законодавстві України, оскільки саме здійснення юридичною особою такого роду операцій дає змогу віднести її до категорії банку, а також відмежувати її від діяльності інших юридичних осіб [10, с. 217]. Це дає підстави стверджувати, що здійснення такого виду діяльності не вимагає отримання банківської ліцензії. У такому разі прийом платежів особами, які за правовим статусом не є банками або фінансовими установами може здійснюватися на підставі агентських відносин, правове регулювання яких здійснюється згідно з главою 31 Господарського кодексу України [11].

Отже, прийом коштів небанківськими установами може здійснюватися на підставі господарських договорів і на даний час не регулюється чинними редакціями Закону України "Про платіжні системи та переказ коштів в Україні" [4] та/або Закону України "Про банки і банківську діяльність" [9].

Вважаємо, що розвиток нових платіжних технологій потребує врегулювання питання широкого функціонального застосування банкоматів або ПТКС з метою надання значно більшого переліку послуг, які можуть надати клієнтам, зокрема введення на рівні Закону поняття та правового режиму використання "ПТКС", можливо шляхом об'єднання (розширення) з поняттям "банківський автомат самообслуговування".

З огляду на викладене Верховній Раді України пропонується внести зміни до Закону України "Про платіжні системи та переказ коштів в Україні" [4] та Закону України "Про банки і банківську діяльність" [9], якими прямо встановити право НБУ регулювати діяльність небанківських осіб щодо прийому готівкових коштів та їх переказ на рахунки третіх осіб.

Щодо усунення можливостей здійснення протиправних діянь, то НБУ як регулятор ринку відслідковує ефективність правозастосування норм, що регулюють застосування нових платіжних технологій. Зокрема є інформація з всесвітньої мережі Інтернет, що в Росії зловмисники викрали ПТКС з місця його розташування, розібрали купюроприймач таким чином щоб однією банкнотою можливо було здійснити безліч платежів на користь інших осіб, а кінцевими вигодонабувачами могли стати самі зловмисники. З огляду на потреби вдосконалення нормативно-правового регулювання та запобігання вчинення шахрайських та інших протиправних дій із використанням як знаряддя злочину ПТКС вважаємо надати наступні рекомендації щодо вдосконалення нормативно-правових актів НБУ. Пропонується покласти на власника ПТКС обов'язок забезпечити:

1) фізичний контроль над місцем знаходження ПТКС, що полягає у закріпленні ПТКС, встановлення вимоги щодо технічної укріпленості накопичувача коштів в готівковій формі ПТКС, постійне радіомаякування ПТКС, заходи щодо забезпечення цілісності каналів зв'язку та інформації, що по них рухається;
2) контролювати режим використання ПТКС в частині періодичності та сум руху коштів;
3) інкасувати кошти з ПТКС, що включає страхування коштів в готівковій формі від крадіжок, встановлення максимальної суми коштів в готівковій формі, що може одночасно перебувати в ПТКС, встановлення періодичності, вилучення коштів в готівковій формі з ПТКС.

Література

1. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність. Навчальний посібник, – К.: Атіка, 2002. – 240 с.
2. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
3. Закон України "Про Національний банк України" // Відомості Верховної Ради України. – 1999, – № 29. – Ст. 238.
4. Закон України "Про платіжні системи та переказ коштів в Україні" // Відомості Верховної Ради України. – 2001. – № 29. – Ст. 137.
5. Постанова Правління Національного банку України від 05.03.2008 № 53 "Про врегулювання питань здійснення операцій із застосуванням програмно-технічних комплексів самообслуговування" // Офіційний вісник України. – 2008. – № 25. – Ст. 800.
6. Закон України "Про фінансові послуги та державне регулювання ринків фінансових послуг" // Відомості Верховної Ради України. – 2002. – № 1. – Ст. 1.
7. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних системам, затверджене постановою Правління від 25.09.2007 № 348 // Офіційний вісник України. – 2007, – № 78. – Ст. 2907.
8. Ліцензійні умови здійснення переказу коштів небанківськими фінансовими установами, затверджені Розпорядженням Держфінпослуг від 23.03.2006 № 5523 // Офіційний вісник України. – 2006. – № 15. – Ст. 1147.
9. Закон України "Про банки і банківську діяльність" // Відомості Верховної Ради України. – 2001. – № 5–6. – Ст. 30.
10. Закон України "Про банки і банківську діяльність": Науково-практичний коментар / За заг. ред. В.С. Стельмаха. – К.: Концерн "Видавничий Дім "Ін-Юре", 2006. – 520 с.
11. Господарський кодекс України // Відомості Верховної Ради України. – 2003. – № 18–22. – Ст. 144.

А.Л. Баланда, *д-р екон. наук, проректор з наукової роботи Національної академії Служби безпеки України*

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ АВТОМАТИЗОВАНИХ СИСТЕМ

Проблема безпеки інформаційних технологій сьогодні набуває особливої актуальності, що зумовлюється, з одного боку, стрімким розвитком інформаційних технологій, з іншого, має місце значне відставання теорії та практики забезпечення безпеки порівняно з динамікою технологічного прогресу [1, с. 3]. Створення глобального інформаційного середовища зумовило можливості доступу до інформаційних ресурсів значної кількості користувачів різної кваліфікації, більшість з яких не мають навичок підтримання безпеки комп'ютерних систем на належному рівні. Тотальна комп'ютеризація банківської системи значно загострила проблему виявлення та протидії новим видам інформаційних загроз, оскільки засоби автоматизованої обробки інформації з використанням персональних комп'ютерів та комп'ютерних мереж мають ряд

особливостей, що дозволяють безконтрольно маніпулювати інформацією відповідних автоматизованих систем як персоналу, так і стороннім особам, а також отримувати несанкціонований доступ до конфіденційної інформації. У зв'язку з цим введення та обробка інформації обмеженого доступу у будь-яких автоматизованих системах повинна враховувати потенційні ризики й супроводжуватися упровадженням відповідних засобів і заходів захисту.

Загрозами інформаційній безпеці банківської автоматизованої системи вважаються фактори, направлені на порушення нормальних умов її функціонування. Вони можуть бути як цілеспрямованими (суб'єктивними), так і випадковими (об'єктивними). Розроблені на сьогодні нормативні стандарти, у більшості випадків, направлені на протидію загрозам суб'єктивного характеру (захист інформації від несанкціонованого доступу), однак не меншу небезпеку функціонуванню автоматизованих систем становлять об'єктивні фактори [2, с. 113]. Так, порушення цілісності даних внаслідок неякісного проектування баз даних може звести нанівець цінність всіх накопичених інформаційних масивів; можлива також повна втрата інформації внаслідок апаратної аварії.

Протидію об'єктивним загрозам можна віднести до питань забезпечення надійності системи. Основним завданням забезпечення інформаційної безпеки є протидія суб'єктивним загрозам. У загальному вигляді види загроз можна класифікувати наступним чином: загрози конфіденційності, загрози цілісності, загрози відмови в обслуговуванні. Проведений аналіз дає змогу виділити основні способи реалізації загроз автоматизованій інформаційній системі: інформаційні, програмно-математичні, фізичні й організаційно-правові.

Під інформаційними способами впливу розуміються різного роду несанкціоноване маніпулювання інформацією, яка знаходиться в базах даних (незаконний доступ до даних, заволодіння і копіювання інформації, її викривлення, порушення технології обробки) [3, с. 27].

Програмно-математичні способи зводяться до введення в систему руйнівних програм чи апаратних пристроїв. Їх призначення полягає в реалізації недокументованих функцій, які призводять до втрати чи псування даних. У зв'язку з тим, що сьогодні в банківській системі використовується виключно імпортне обладнання та програмне забезпечення, ймовірність впровадження спеціальних "закладок" є досить високою. Більш того, такі випадки зустрічаються все частіше.

Фізичні способи впливу здійснюються через фізичну дію різних факторів на комп'ютерну техніку, мережі, носії інформації, а також на персонал, який працює з конфіденційною інформацією, та охоронні

системи. Так, за оцінками Асоціації захисту інформації США біля 40 % причин збоїв у роботі комп'ютерних систем викликані фізичними загрозами. Фізичний вплив може організовуватися і за допомогою високотехнологічної електронної апаратури, яка може перехоплювати сигнали від працюючого обладнання і таким чином викрадати інформацію. Можливим також є блокування сигналів та порушення нормального функціонування обладнання, введення пристроїв перехоплення інформації в робочих приміщеннях. Не менш ефективним засобом знищення інформаційної бази можуть стати найпростіші руйнівні впливи: пожежа чи залиття обладнання водою, причому достатньо організувати пожежу у сусідньому приміщенні, куди доступ сторонніх є спрощеним. Менш очевидними, але досить ефективними є організаційно-правові способи впливу загроз (невиконання персоналом вимог нормативних документів, затримка з прийняттям відповідних нормативно-правових положень).

Попередження, мінімізація чи нейтралізація загроз інформаційній безпеці здійснюється за допомогою засобів захисту інформації на основі розроблених і упроваджених методів протидії різного роду загрозам інформаційній безпеці [4]. Під засобами захисту інформації розуміються організаційні, технічні, криптографічні, програмні засоби, призначені для захисту інформації з обмеженим доступом, а також програмні засоби й спеціальна техніка, в яких вони реалізовані. До них можна віднести також і засоби контролю ефективності захисту інформації. Для ефективного і комплексного захисту інформації необхідне використання різних методів протидії загрозам, а також запобігання самій можливості їх впливу. Серед заходів протидії загрозам інформаційній безпеці банківських автоматизованих систем можна виділити: виключення несанкціонованого доступу до інформації, запобігання спеціальних впливів, направлених на руйнацію, знищення, викривлення інформації чи збої в роботі засобів інформатизації; виявлення впроваджених програмних чи апаратних закладних пристроїв; застосування засобів захисту від витоків інформації по технічним каналам; застосування засобів захисту інформації, у тому числі криптографічних, при передачі по каналам зв'язку.

В процесі планування протидії цілеспрямованим загрозам інформаційній безпеці банківських автоматизованих систем слід враховувати той факт, що хоча й атаки ззовні на комп'ютерні системи широко обговорюються й викликають підвищену зацікавленість, однак незрівнянно більшу шкоду безпеці приносять порушення всередині банківської установи. Вимоги інформаційної безпеки зачіпають інтереси практично всіх співробітників банку. Ситуація ускладнюється тим, що, поряд зі своїми основними посадовими обов'язками, ці співробітники повинні

виконувати часто незрозумілі і тому неприйнятні функції й процедури, пов'язані вимогами безпеки. Причинами цього може бути низька кваліфікація персоналу, недостатня для коректної роботи з базами даних чи недбалість. Особливо небезпечними є некомпетентні співробітники, які видають себе за досвідчених користувачів. За відсутності в банківській установі контролю за встановленням на робочих місцях програмного забезпечення співробітник може інсталювати на свій комп'ютер неліцензійну програму, навіть не розуміючи можливих наслідків. Аналогічна загроза виникає і у випадку підключення робочої станції до мережі Інтернет через модем. Загрозу становить також практика обміну паролями між співробітниками, які виконують споріднені функції чи залишення занотованих паролів на робочих місцях.

Широке розповсюдження мобільних накопичувачів інформації обумовило появу нового класу загроз інформаційній безпеці банківських автоматизованих систем. Проблема несанкціонованого використання таких пристроїв не завжди може вирішуватися заходами організаційного захисту інформації і може призвести до витікання інформації. Єдиною альтернативою фізичному відключенню USB-портів на робочих місцях може бути лише використання спеціальної системи захисту. Окремі комп'ютери, навіть не підключені до локальної мережі, потребують дотримання особливих правил безпеки, у разі коли на них обробляються конфіденційні дані. Для захисту локальних комп'ютерів від несанкціонованого доступу повинен застосовуватися комплекс організаційних і технічних заходів, який реалізує чіткий регламент обробки конфіденційної інформації. Засобами реалізації технічних заходів можуть стати аутентифікація користувача, шифрування файлової системи, програмно-апаратні комплекси захисту інформації від несанкціонованого доступу.

Дієвим заходом попередження фізичних загроз банківським автоматизованим системам може стати упровадження окремої комплексної комп'ютеризованої системи управління фізичним захистом об'єкта, яка створюється на базі локальної мережі і об'єднує сервери управління підсистемами, автоматизовані робочі місця та сервери баз даних. Така автоматизована система розрахована на різнопрофільних користувачів і містить інформацію різного ступеня конфіденційності. Наприклад, робоче місце співробітника бюро перепусток повинне забезпечувати доступ лише до необхідних персональних даних співробітників, а робоче місце оператора охорони – до графічних планів об'єкта з даними про розташування засобів охоронної сигналізації У першому випадку інформація носить відкритий характер, у другому – конфіденційний, а, відповідно, й персонал, який працює з даними повинен мати різні рівні допуску.

Таким чином захищена банківська автоматизована система повинна забезпечувати інформаційну безпеку і відповідати наступним вимогам: мати можливості автоматизації процесу обробки конфіденційної інформації, включаючи всі аспекти, пов'язані із забезпеченням безпеки оброблюваної інформації; успішно протистояти загрозам безпеці, які характерні для визначеного середовища; задовольняти прийняті стандарти інформаційної безпеки; забезпечувати безпеку інформації без суттєвого ускладнення функцій користувача. Для попередження загроз інформаційній безпеці та усунення їх негативних наслідків необхідне упровадження комплексу організаційних, правових, технічних і технологічних заходів, які у сукупності повинні запобігати небажаний доступ до апаратури, інформаційних масивів та програмному забезпеченню.

Література

1. Преступления, связанные с использованием компьютерной сети. Справочный документ для семинара-практикума по использованию компьютерной сети / Десятый Конгресс ООН. – Документ ООН. A/CONF/187/10.
2. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями. – М. : Мир, 1999. – 351 с.
3. Цимбалюк В. Організація та координація боротьби з організованою транскордонною кіберзлочинністю // Право України. – 2003. – № 2. – С. 26–30.
4. Петренко С. Методические основы защиты информационных активов компании. Електронний ресурс. Режим доступу: http://citforum.ru/security/articles/ zahita_ aktivov/.

А.В. Бєгун, *доц.*
Київського національного економічного університету ім. Вадима Гетьмана;
В.К. Галіцин, *проф.*
Київського національного економічного університету імені Вадима Гетьмана

ПРО ОДНУ ЗАДАЧУ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ БАНКУ

На сьогодні важливим напрямом підвищення ефективності функціонування багатьох як вітчизняних, так і закордонних банківських інформаційних систем (БІС) є інтеграція з глобальною мережею Інтернет. В багатьох випадках завдяки цієї інтеграції вирішуються дві основні задачі. По-перше, об'єднуються територіально розподілені підсистеми. По-друге, користувачам Інтернету забезпечується доступ до відкритої інформації БІС. Досить часто при вирішенні обох задач використовується Web-сайт, який, крім того, відіграє представницьку роль БІС в Інтернеті. Практичний досвід вказує, що робота Web-сайту значною мірою впливає на ефективність функціонування всієї АІС. Основою Web-сайту є Web-сервер, який забезпечує доступ клієнтів із мережі

Інтернету до Web-сторінок сайту. Важливим є також передача особистих даних користувачів банку.

Останнім часом зафіксовані непоодинокі випадки масованих атак порушників на БІС зі сторони Інтернету, причому досить часто об'єктом таких атак був Web-сервер. Наприклад, за матеріалами CyberSecurity більш 30 % свого часу висококваліфіковані IT-фахівці витрачають на мережеву безпеку. Як правило, наслідками більшості успішних атак на Web-сервер ставало унеможливлення санкціонованого доступу, порушення цілісності або створення неконтрольованого поширення інформації БІС. Таким чином у багатьох випадках успішна атака на Web-сервер може призвести не тільки до загрози функціонування Web-сайту, але й до значного зменшення ефективності функціонування всієї БІС. Цим визначається актуальність запропонованого дослідження – ефективність захищеності інформаційних ресурсів, а також її зв'язок з глобальною науково-практичною проблемою – забезпечення інформаційної безпеки БІС.

Для формалізації задачі оцінювання ефективності системи захисту ін. формаційних ресурсів БІС пропонується наступний підхід. Будемо розглядати систему захисту у вигляді багаторівневої ієрархії I_p, де p – кількість рівнів. Для інформаційних ресурсів на кожному p-му рівні ієрархії вибирається множина об'єктів захисту M_{kp}, де k – номер об'єкта на p-му рівні. За допомогою експертного оцінювання для кожного M_{kp} об'єкта формується вектор загроз V_{skp}, де s – номер загрози для k-го об'єкта на p-му рівні ієрархії. Зниження ефективності використання інформаційного ресурсу на кожному p-му рівні ΔE_p визначається складним впливом реально діючих загроз на об'єкти p-го рівня:

$$\Delta E_p(t) = F\left\{M_{kp}, V_{skp}, t\right\}, \qquad (1)$$

де $F\{*\}$ – функціонал, що описує вплив реально діючих загроз V_{skp} на множину об'єктів M_{kp} в підсистемі p-го рівня;

t – часова характеристика. При цьому вважається, що відновлення ефективності підсистеми p-го рівня можливо лише завдяки проведенню адекватного рівню інтегральної загрози комплексу заходів безпеки Z_{jkp}, де j – номер заходу безпеки Z стосовно k-го об'єкта підсистеми p-го рівня.

Пропонується поставити в залежність кількісну оцінку рівня інтегральної загрози $IC(U)$ від зниження ефективності БІС (ΔE) в цих умовах. Таким чином, враховуючи (1), у формалізованому виді рівень інтегральної загрози БІС на момент *t* можна оцінити функціоналом (2) з урахуванням обмежень (3):

$$U(t) = F\{M_{kp}, V_{skp}, t\}; \tag{2}$$

$$0 \le U(t) \le 1, \tag{3}$$

де $U(t) = 0$ – означає повну відсутність загрози для АІС;

$U(t) = 1$ – вивід з ладу БІС (ефективність БІС дорівнює 0).

Оцінку рівня загрози деякому *k*-му об'єкту БІС рекомендується здійснювати за сукупністю окремих показників U_{kn} для відповідного об'єкта. Кожний *n*-й показник відображає події, які пов'язані із зростанням загрози використання інформаційного ресурсу БІС *p*-го рівня. Формулу (2) рекомендується проводити шляхом часткових розрахунків $U(t)$ у фіксовані моменти часу *t* на основі використання методу аналізу ієрархій, а потім за окремими точками встановлюють функціональну залежність, яку можна використовувати у подальшому для прогнозування зміни рівня інтегральної загрози з плином часу.

Запропонований підхід оцінки ефективності захисту БІС є досить досконалим та універсальним, але потребує уточнення та деталізації при оцінці ефективності захисту конкретної БІС, а в нашому випадку Web-серверу. Також відомі нормативні вимоги до системи захисту Web-серверів від несанкціонованого доступу (НСД). Це дозволяє з урахуванням нормативних вимог на базі формул (1–3) провести оцінку ефективності захисту найбільш розповсюджених Web-серверів від НСД. Зазначимо, що визначення такої оцінки в доступній нам літературі не знайдено.

Важливим результатом наведеної роботи є кількісні та якісні показники ефективності захисту Web-серверу Apache від атак на відмову. Але для повноти результатів необхідно провести порівняння аналогічних показників ефективності захисту для різних типів Web-серверів, наприклад для Apache та IIS.

Нагадаємо: найбільш важлива Web-сторінка (Web-сайт) – це мережевий інформаційний ресурс, наданий користувачеві у вигляді HTML-документа з унікальною адресою у мережі; сервер (server) – об'єкт

комп'ютерної системи (програмний або програмно-апаратний засіб), що надає послуги іншим об'єктам за їх запитами. Web-сервер обслуговує запити користувачів (клієнтів) згідно з протоколом http (Hyper Text Transfer Protocol), забезпечує актуалізацію, збереження інформації Web-сторінки, зв'язок з іншими серверами.

Використавши співвідношення (1–3), інтегральну оцінку ефективності захисту Web-серверів $(Z_w(t))$ можна провести наступним чином

$$Z_w(t) = F\{Z_{wi}, V_i, t\}, \tag{4}$$

де V_i – загроза за номером i;

Z_{wi} – ефективність заходу безпеки від загрози V_i;

t – часова характеристика.

Припустимо, що термін реалізації загроз та відповідних їм заходів безпеки незначний. Це дозволяє знехтувати впливом часових характеристик на ефективність захисту. Таким чином, оцінку ефективності захисту можна розрахувати як

$$Z_w = F\{Z_{wi}, V_i\}. \tag{5}$$

Крім того, в першому наближені можна прийняти, що величина Z_{wi} детермінована і може набувати тільки два значення: 0 – захід неефективний та 1 – захід ліквідує загрозу. Розглянемо випадок визначення інтегральної оцінки захисту Web-серверів від НСД. У цьому випадку відомий перелік нормативних заходів безпеки, що дозволяє переписати функціонал (5) у наступному вигляді:

$$Z_w = \sum_{i=1}^{N} Z_{wi},$$

де i – номер заходу безпеки;

N – нормативна кількість заходів безпеки.

Очевидно, що мінімальна величина $Z_w = 0$, а максимальна – $Z_w = N$. При $Z_w = 0$ захист абсолютно неефективний з точки зору відповідності нормативам. При $Z_w = N$ захист повністю відповідає нормативним заходам безпеки.

А.І. Марущак, *д-р юрид. наук, доц., перший заступник директора Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України*

ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВСЬКОЇ УСТАНОВИ: СТРУКТУРА ТА СИСТЕМА ЗАБЕЗПЕЧЕННЯ

Структурно інформаційну безпеку банківських установ складають:

- безпека інформаційних ресурсів; безпека інформаційної інфраструктури та безпека "інформаційного поля" підприємства.

Інформаційні ресурси банківської установи – це взаємозв'язана, упорядкована, систематизована і закріплена на матеріальних носіях інформація, яка належить банківській установі. Відповідно *безпека інформаційних ресурсів* полягає у збереженні такої інформації від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності).

Безпека інформаційної інфраструктури полягає у такому стані захищеності електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку банківської установи, яка забезпечує цілісність і доступність інформації, що в них обробляється (зберігається чи циркулює).

Безпека "інформаційного поля" банківської установи складається здебільшого з несистематизованих потоків інформації, що оприлюднюється різноманітними учасниками інформаційних відносин: телерадіоорганізаціями, друкованими ЗМІ, Інтернет-виданнями, конкурентами, органами державної влади, місцевого самоврядування тощо.

Найбільш суттєвими загрозами безпеки інформаційних ресурсів є витік або втрата таких ресурсів (зокрема відомостей, що становлять банківську таємницю). Загрози інформаційним ресурсам можуть бути реалізовані шляхом:

- підкупу осіб, які мають безпосередній доступ до банківської таємниці та іншої інформації з обмеженим доступом банківської установи;
- необережного, недбалого поводження з банківською таємницею та іншою інформацією з обмеженим доступом;
- недотримання вимог збереження інформації з обмеженим доступом, встановлених у банківській установі, при контактах з контролюючими і наглядовими органами внаслідок правової та психологічної непідготовленості відповідальних працівників банківської установи тощо.

Протидія таким загрозам має полягати, насамперед, у:

- визначенні надійності працівників підприємства, які працюватимуть з банківською таємницею та іншою інформацією з обмеженим доступом;
- організації спеціального діловодства з відомостями, що становлять та інформацію з обмеженим доступом банківської установи;

- обґрунтуванні і закріпленні диференційованого доступу працівників до банківської таємниці та іншої інформації з обмеженим доступом, при якому працівник може ознайомлюватися і вчиняти певні дії з нею виключно для виконання покладених на нього функціональних обов'язків;
- закріпленні персональної відповідальності працівника за збереження наданих йому або розроблених ним документів, інших носіїв інформації, що містять інформацію з обмеженим доступом банківської установи;
- обмеженні доступу працівників і сторонніх осіб до приміщень, у яких обробляється (зберігається) інформація з обмеженим доступом банківської установи;
- впровадженні заходів контролю за роботою працівників з носіями інформації з обмеженим доступом банківської установи, а також ефективної системи виявлення і фіксації протиправних діянь з такою інформацією;
- впровадженні надійної і ефективної системи зберігання носіїв інформації, що виключає несанкціоноване ознайомлення з ними, їх знищення чи підробку.

Суттєвими загрозами безпеки інформаційної інфраструктури є:

- неофіційний доступ та зняття інформації, що охороняється, технічними засобами;
- перехоплення інформації, що циркулює в засобах і системах зв'язку та обчислювальної техніки, за допомогою технічних засобів негласного зняття інформації, несанкціонованого доступу до інформації та навмисних технічних впливів на них в процесі обробки та зберігання;
- підслуховування з використанням технічних засобів конфіденційних переговорів, що ведуться в службових приміщеннях, автотранспорті тощо.

Протидія таким загрозам має полягати, насамперед, у широкому і головне економічно доцільному застосуванні технічних засобів безпеки інформаційної інфраструктури.

Конкретними заходами ліквідації загроз безпеці інформаційної інфраструктури банківської установи мають бути:

- створення цілісності засобів захисту, технічного і програмного середовища, що полягає у фізичному збереженні засобів інформатизації, незмінності програмного середовища, виконанні засобами захисту передбачених функцій, ізольованості засобів захисту від користувачів;
- захист інформації від витоку внаслідок наявності фізичних полів за рахунок акустичних та побічних електромагнітних випромінювань і наводок на комунікаційні мережі та конструкції будівель;

- використання криптографічного захисту найбільш цінної інформації при її обробці в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку підприємства;
- надання диференційованого доступу працівникам для здійснення конкретних операцій (створення, читання, запис, модифікація, видалення) за допомогою програмно-технічних засобів, а також розмежування доступу користувачів до даних в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку банківської установи різного рівня та призначення;
- ідентифікація користувачів та здійснюваних ними процесів в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку установи на основі використання паролів, ключів, магнітних карт, цифрового підпису, а також біометричних характеристик особи як при доступі до інформаційно-телекомунікаційних систем;
- реєстрація (з фіксацією дати і часу) дій користувачів з інформаційними та програмними ресурсами в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах, зокрема протиправних спроб доступу;
- попередження передачі інформації з обмеженим доступом по незахищених лініях зв'язку;
- запобігання впровадженню в інформаційно-телекомунікаційні системи програм-вірусів;
- регулярна перевірка технічних засобів і приміщень для виявлення наявності в них пристроїв несанкціонованого доступу до інформації;
- обладнання спеціальних приміщень для захисту мовної інформації при проведенні конфіденційних переговорів тощо.

Найбільш суттєвими загрозами безпеки "інформаційного поля" є підрив ділового іміджу банківської установи, виникнення проблем у взаємостосунках з реальними та потенційними клієнтами, конкурентами, контролюючими та правоохоронними органами, викликаних насамперед поширенням недостовірної, заздалегідь неправдивої інформації про банківську установу, здійсненням негативних інформаційних впливів на його керівництво, працівників тощо.

Конкретними заходами ліквідації загроз безпеці "інформаційного поля" банківської установи мають бути:

- створення досконалої інформаційно-аналітичної діяльності;
- оперативне реагування на випадки поширення неправдивої інформації про банківську установу;

- скоординоване і централізоване поширення рекламної, маркетингової та іншої інформації, що підвищує імідж і сприйняття банківської установи клієнтами;
- налагодження у межах чинного законодавства інформаційної співпраці з органами державної влади і місцевого самоврядування.

Таким чином, система забезпечення інформаційної безпеки банківської установи полягає у створенні комплексу організаційних, технічних, програмних і криптографічних засобів і заходів задля:

- захисту інформації з обмеженим доступом банківської установи від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності);
- забезпечення цілісності і доступності інформації, що обробляється, зберігається, циркулює в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку банківської установи;
- протидії поширенню недостовірної, заздалегідь неправдивої інформації про банківську установу, здійсненню негативних інформаційних впливів на її керівництво.

Література

1. Закон України "Про банки і банківську діяльність" від 07.12.2000 року // Відомості Верховної Ради України. – 2001. – № 5–6. – Ст. 30.
2. Закону України "Про електронні документи та електронний документообіг" від 22 травня 2003 року // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.
3. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту // Правова інформатика. – 2009. – № 1. – С. 64–70.

А.С. Щепинов, *ст. преподаватель кафедры программирования Московского государственного университета имени М.В. Ломоносова*

НЕКОТОРЫЕ ОСОБЕННОСТИ РЕЖИМА ШИФРОВАНИЯ CBC

Рассматривается режим блочного шифрования CBC, широко используемый для криптозащиты массивов данных, размерность которых превышает размер блока алгоритма шифрования. Показано, что для некоторых значений вектора инициализации, ключа шифрования и значения шифруемых данных зашифрованный массив целиком или частично совпадает с исходным. Используя, известное свойство сопряжения подстановок этот недостаток устраняется в режиме CBC.

В режиме сцепления блоков шифра (Chiphtr Block Chaining, CBC) [1, 2] массив данных $X = (x_1, x_1, \ldots, x_k)$ длины $k \cdot l$ бит разбивается на k блоков по l бит в каждом. Блоки исходного массива x_i последовательно,

начиная с первого, преобразуется в блоки y_i зашифрованного массива $Y = (y_1, y_1, \ldots, y_k)$ путем поразрядного сложения по модулю два вектора сцепления y_{i-1}, равного зашифрованному значению предыдущего блока, со значением блока x_i. После этого производиться шифрование полученной суммы алгоритмом E – алгоритмом шифрования блоков длины l бит. Значение y_{i-1} блока зашифрованного на предыдущем шаге называют вектором сцепления блоков.

$$y_i = E(y_{i-1} + x_i) \quad i = 1, 2, \ldots, k. \tag{1}$$

Здесь и и далее знак + обозначает поразрядное сложение по модулю два. Для шифрования первого блока

$$y_i = E(y_0 + x_i) \tag{2}$$

используется код y_0 длины l, который называют вектором инициализации [3]. В выражениях (1), (2) и далее знак + обозначает поразрядную сумму по модулю 2 двоичных векторов длины l. Алгоритм шифрования блоков длины l реализует взаимно однозначную функцию (перестановку) E на множестве из всех 2^l значений двоичных векторов длины l. Перестановка E определяется ключом шифрования, который сохраняется в секрете от несанкционированного пользователя. Операция поразрядного сложения по модулю 2, для фиксированного значения y_{i-1}, является перестановкой [4, 130–134] на множестве двоичных векторов длины l. Схема реализации режима шифрования CBC показана на рисунке 1.

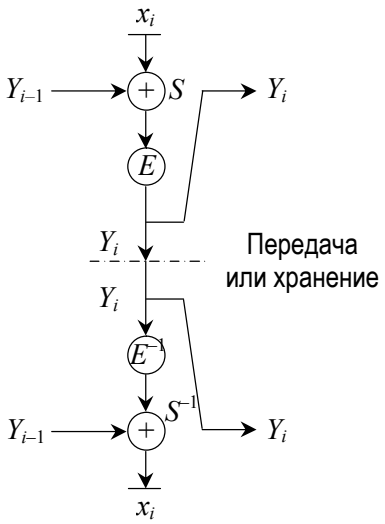


Рис. 1. Реализация режима блочного шифрования CBC

Для шифрования блока x_i выполняется композиция $S \cdot E$ функций сложения по модулю два S и шифрования E. С учетом того, что операция сложения по модулю два S обратна самой себе, для расшифрования зашифрованного блока y_i [5, 219] выполняются обратные операции в обратном порядке $E^{-1} \cdot S^{-1} = E^{-1} \cdot S$. Для обеспечения конфиденциальности передаваемой или хранящейся в режиме CBC информации ключ шифрования, определяющий E и вектор инициализации передается по защищенному каналу связи.

Рассмотрим процесс получения зашифрованного значения блока x_i массива X алгоритмом шифрования E (1) в режиме CBC. Для любого значения первого блока x_i существует опасное значение вектора сцепления y_{i-1}, для которого

$$x_i = E\left(y_{i-1} + x_i\right). \tag{3}$$

Действительно, так как левая и правая часть (3) представляют собой один и тот же двоичный вектор знак равенства сохраниться, если выполнить дешифрование левой и правой части.

$$E^{-1}\left(x_i\right) = E^{-1}\left(E\left(y_{i-1} + x_i\right)\right).$$

Учитывая групповые свойства подстановок [5, 218] выражение преобразуется в

$$E^{-1}\left(x_i\right) = y_{i-1} + x_i, \tag{4}$$

а учитывая свойства операции поразрядного сложения по модулю 2, из (4) следует, что такое опасное значение вектора сцепления определяется из выражения

$$y_{i-1} = E^{-1}\left(x_i\right) + x_i. \tag{5}$$

Если подставить полученное в (5) опасное значение y_i в (2), то получим

$$y_1 = E\left(x_1 + E^{-1}\left(x_1\right) + x_1\right) \quad E\left(E^{-1}\left(x_1\right)\right) \quad x_1$$

откуда следует, что если выполняется (5), то первый блок зашифрованного массива y_1 равен первому блоку исходного массива x_1. Кроме этого, если для некоторого или всех $i = 2, 3, \ldots, k$ выполняется условие (5), то подставив (5) в (1) получим

$$y_i = E\left(y_{i-1} + x_i\right) = E\left(E^{-1}\left(x_i\right) + x_i + x_i\right) = E\left(E^{-1}\left(x_i\right)\right) \quad x_i$$

каждый *i*-й зашифрованный блок, для которого выполняется (5), равен одноименному блоку исходного массива. Обнаруженные недостатки устраняются, если выполнять шифрование блока массива данных *X*, используя схему

$$y_i = y_{i-1} + E\left(y_{i-1} + x_i\right), \tag{6}$$

в которой после выполнения шифрования поразрядной суммы блока данных x_i и вектора сцепления y_{i-1}, полученный результат вновь поразрядно складывается по модулю два с вектором сцепления. Действительно, пусть для шифрования используется алгоритм *E*, который шифрует любые значения блоков данных *x* так, что

$$E\left(x\right) \neq x. \tag{7}$$

Такие перестановки называют беспорядками. Предположим, что для некоторых значений блока x_i и вектора сцепления y_{i-1} выполняется условие (блок не шифруется)

$$x_i = y_{i-1} + E\left(y_{i-1} + x_i\right).$$

Тогда, с учетом свойств операции поразрядного сложения по модулю 2.

$$x_i + y_{i-1} \quad E\left(y_{i-1} + x_i\right),$$

что невозможно, если выполняется условие (7). На рисунке 2 изображена схема реализации модернизированного режима шифрования CBC.

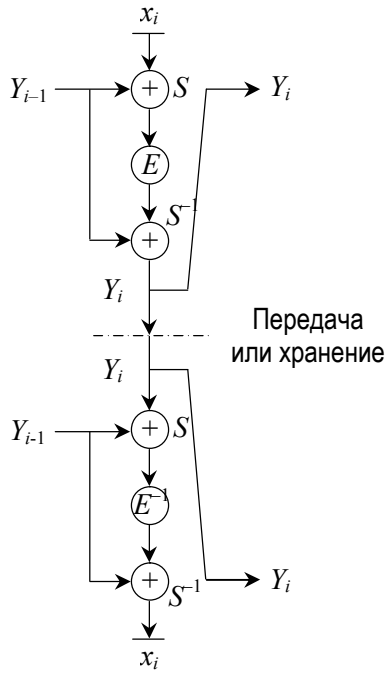


Рис. 2. Усовершенствованная схема шифрования в режиме CBC

В этой схеме шифрование выполняется композицией перестановок SES^{-1}. Полученная композиция функций SES^{-1} называется сопряжением подстановки E посредством подстановки S. В [6, 234–237] показано, что сопряжение SES^{-1} сохраняет цикловую структуру перестановки E. Поэтому, если алгоритм блочного шифрования E является беспорядком (7), то беспорядком будет и сопряжение подстановок SES^{-1}. Поэтому любые значения вектора сцепления в схеме шифрования показанной на рисунке 2 являются безопасными.

Литература

1. ANSI. American National Standard X3.106: Data Encryption Algorithm. Mode of Operations. 1983.
2. ISO 8372. Information Processing Systems: Data Encripherment: Modes of Operation of 64-bit Block Cipher.
3. Деднев М.А., Дыльнов Д. В., Иванов М.А. Защита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-ОБРАЗ, 2004, 512 с.
4. Щепинов А.С. Кирдякина Е.А Программная реализация подстановок. Збірник наукових праць Академии вийсково-морських сил імени П.С. Нахимова. Выпуск 1(1) Севастополь 2010 г. 130–134.
5. Г. Биркгоф, Т. Барти. Современная прикладная алгебра. Пер. с английского. М. “Мир”. 1976 г. 269 с.
6. Щепинов А.С. Реализация одноцикловых подстановок. Информационные технологии и информационная безопасность в науке технике и образовании “ИНФОТЕХ-2004”. Материалы международной научно-практической конференции. Киев–Севастополь.: НТО РЭС Украины. 2004 г. С. 234–237.

И.В. Куржеевский, *ст. преподаватель кафедры защиты информации Академии военно-морских сил имени П.С. Нахимова*

СТОХАСТИЧЕСКИЙ БЛОЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ

Любую операцию, используемую при построении блочных шифров, можно представить как отображение векторного пространства h-мерных двоичных векторов $W = (w_1, w_2, \ldots, w_h)$ в векторное пространство n-мерных двоичных векторов $Y = (y_1, y_2, \ldots, y_n)$, где для всех $j \in \{1, \ldots, h\}$ и $i \in \{1, \ldots, n\}$ имеем $w_j, y_i \in GF\ (2)$. Обычно в управляемых операциях можно выделить информационный вход и управляющий вход. Отображаемый вектор W длины h представляется в виде конкатенации (X, V) преобразуемого вектора Y длины N и управляющего вектора V длины $m = h - n$.

Одним из видов управляемых операций являются операции битовых перестановок в зависимости от преобразуемых данных. Битовая перестановка, зависящая от ключа, остается строго линейной операцией, поскольку она является фиксированной после ввода ключа. Принципиально ситуация изменяется, когда перестановка является переменной операцией, т. е. в случае ее выполнения в зависимости от значения преобразуемого блока данных, которое по своей природе является переменной величиной.

Вопросы проектирования криптосистем на основе управляемых операций рассмотрены в [1–3]. Одним из типов управляемых операций являются операции, зависящие от преобразуемых данных. Их особенностью является изменчивость реализуемых модификаций, что позволяет использовать термин “переменные операции”. Различные аспекты создания управляемых битовых перестановок рассмотрены в [2]. Очевидно, что перестановка, зависящая от преобразуемых данных, описывается как операция подстановки частного вида, выполняемая над всем преобразуемым блоком данных и оставляющая управляющий вектор без изменения.

В работе предложенного авторами блочного алгоритма шифрования на основе стохастических битовых перестановок, управляемых данными, и случайного выбора булевых функций из множества инволюнтных функций можно выделить четыре этапа.

1. Генерация случайных бит и их “перемешивание” с информационными.

2. Осуществление первичной стохастической перестановки бит по случайному закону, определяемому генератором псевдослучайных последовательностей (ГПСП).

3. Шифрование блока бит с использованием булевых инволюнтных функций.

4. Осуществление вторичной стохастической перестановки бит по случайному закону, определяемому ГПСП.

Вышеперечисленные четыре этапа составляют один раунд процесса шифрования. Количество раундов задается в зависимости от требований к защищенности информации. “Подмешивание” случайных бит является одной из главных особенностей алгоритма и вносит значительную долю неопределенности в получаемый шифр-текст. Характерным является тот факт, что доля случайных бит в шифруемом блоке информации непостоянна и определяется случайным образом при помощи генератора псевдослучайных последовательностей, что повышает, по мнению авторов, криптостойкость зашифрованной информации. В качестве случайных бит выступают биты, полученные при помощи генератора псевдослучайных последовательностей на основе бент-функции. Булева бент-функция используется для усложнения структуры псевдослучайной последовательности в комбинирующем генераторе на вход которого в качестве значений аргументов поступают биты от различных генераторов на основе регистров сдвига с линейными обратными связями.

Данный этап алгоритма шифрования реализуется в следующей последовательности:

1. Выбирается длина блока шифруемых данных N.
2. С помощью ГПСП № 1 с ключем $K1$ генерируется случайное число l-количество информационных бит в блоке.

Количество информационных бит выбирается так, чтобы оно не превышало заранее определенного значения. Обычно количество информационных бит составляет примерно половину величины блока. Значение этого параметра напрямую влияет на криптостойкость зашифрованной информации, чем меньше доля информационных бит, тем сложнее взломать данный шифр.

3. Происходит заполнение блока данных информационными битами в количестве l-битов.

4. Оставшиеся позиции в блоке данных дополняется случайными битами, сгенерированными при помощи генератора на основе бент-функции (ГПСП № 2) и определяется как $N - l$.

Полученный блок данных поступает на следующий этап шифрования – стохастическую перестановку.

По закону, определяемому ГПСП № 3 с ключом $K3$, осуществляется стохастическая перестановка бит в блоке данных с использованием контрольного массива. Процесс продолжается до тех пор, пока не

будут считаны все биты блока данных. Полученный массив данных поступает на следующий этап шифрования. На данном этапе осуществляет шифрование групп бит при помощи множества сбалансированных инволюнтных БФ от трех переменных, случайным образом выбранных из 764 вариантов [2]. Номер варианта определяется работой ГПСП № 4 с ключом $K4$. В процессе шифрования используется управляющий вектор, значения которого определяются работой ГПСП № 5 с ключом $K5$. Полученный в результате шифрования инволюнтными БФ блок данных подвергается вторичной стохастической перестановке. Данный этап полностью эквивалентен первичной перестановке, с той лишь разницей, что используется ГПСП № 6 с ключом $K6$ для стохастического размещения бит в массиве данных. Процесс расшифрования происходит в обратном порядке.

Рассмотрим комбинаторные методы оценки криптостойкости разработанного алгоритма шифрования. Данные методы служат для оценки сложности взлома того или иного алгоритма шифрования и как правило справедливы для случая атаки шифра “в лоб” или по-другому методом “грубой силы” (brute force). Суть данного метода состоит в подсчете числа возможных комбинаций, которые необходимо перебрать злоумышленнику для взлома.

Для разработанного алгоритма криптостойкость обеспечивается за счет “подмешивания” случайных бит в исходных текст и последующей их стохастической перестановки посредством генератора ПСП. Здесь криптостойкость напрямую зависит от размера блока данных и качества ГПСП.

Предположим, что мы выбрали размер блока данных равным 512 бит. Среди этих 512 бит будут как случайные, так и информационные биты. Количество их определяется с помощью ГПСП № 1 и заранее неизвестно. Пусть количество информационных бит находится в пределах от $1/4$ до $1/2$ длины блока данных, что соответствует минимальной и максимальной криптостойкости и составляет 128 и 256 бит. Так как заранее установить количество 0 и 1 практически невозможно, то будем считать их примерно одинаковым. Использую формулу для числа перестановок с повторениями, получим количество вариантов, необходимых для полного перебора:

$$P_{\max} = \frac{512!}{256! \cdot 256!} \approx 4,72 \cdot 10^{152}.$$

$$P_{\min} = \frac{512!}{384! \cdot 128!} \approx 4,46 \cdot 10^{123}$$

для случаев максимального и минимального содержания случайных бит в блоке соответственно. Исходя из этих значений, можно сделать вывод, что стохастические перестановки с “подмешиванием” случайных бит, реализованные в данном алгоритме повышают стойкость к методам взлома на основе полного перебора. Данный алгоритм был реализован на языке C++ в среде Borland C++ Builder 6.0 и показал свою работоспособность.

Криптостойкость предложенного авторами блочного алгоритма шифрования на основе стохастических битовых перестановок, управляемых данными, основывается на выборе булевых функций, строение которых (сбалансированность, соответствие показателям корреляционной иммунности, критериям строгого лавинного эффекта, низкие автокорреляционные значения и высокая нелинейность) обеспечивает стойкость к методам линейного и дифференциального криптоанализа. Стохастические перестановки с “подмешиванием” случайных бит повышают стойкость к методам взлома на основе полного перебора. Данный алгоритм можно рекомендовать в качестве алгоритма предварительного шифрования информации при использовании криптографически стойких генераторов псевдослучайных последовательностей на основе бент-функций как для выбора сбалансированных инволюнтных БФ из 764 вариантов, так и для генерации битов управляющего вектора, случайных бит и псевдослучайных чисел, необходимых для стохастических перестановок.

Литература

1. Молдовян Н.А. Скоростные блочные шифры / Н.А. Молдовян. – СПб : СПбГУ, 1998. – 230 с.
2. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб.: БХВ – Петербург, 2004. – 448 с.
3. Moldovyan A.A. A cipher based on data-dependent permutations / A.A. Moldovyan, N.A. Moldovyan // Journal of Cryptology. 2002. Vol. 15. – pp. 61–72.

А.А. Гордеев, *канд. техн. наук,*
заведующий кафедрой математики и социально-гуманитарных дисциплин
Севастопольского института банковского дела
Украинской академии банковского дела НБУ

СЕТЕВЫЕ АКАДЕМИИ CISCO: ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО КОМПЬЮТЕРНЫМ СЕТЯМ

Каждая компания-производитель активного сетевого оборудования стремится к расширению своего рынка. Конкуренция среди таких компаний является достаточно высокой, однако бесспорным лидером

в данном сегменте рынка является компания Cisco Systems, Inc. Одним из определяющих факторов, определивших такой уровень компании на рынке, является создание и динамичное развитие образовательного направления – формирование сетевых академий, на базе которых проводится подготовка специалистов по сетевым технологиям Cisco.

Сетевые академии Cisco являются развитой образовательной сетью, поскольку насчитывают порядка 9 000 академий в 165 странах мира. Образовательные программы сетевых академий Cisco достаточно разнообразны и включают подготовку специалистов по следующим основным направлениям:

- проектирование сетей (Cisco Certified Design Associate – CCDA);
- маршрутизация и коммутация (Cisco Certified Network Associate – CCNA Routing and Switching);
- безопасность компьютерных сетей (CCNA Security);
- передача голоса по IP-сетях (CCNA Voice);
- беспроводные сети (CCNA Wireless).

Каждый курс разбит на ряд связанных тематических семестров. Схема обучения для каждого из них является унифицированной и содержит следующие составляющие обучения:

- теоретический материал, представленный в виде мультимедийных презентаций;
- практические задания, выполнение которых предусматривает применение реального оборудования Cisco;
- тестирование по теоретическим знаниям и практическим навыкам. Стоит отметить, что тестирование проводится после каждого семестра (семестровые тесты), а также в конце каждого курса (финальные тесты). По итогам прохождения тестирования в случае успешного результата студент получает сертификат, подтверждающий то, что он прослушал курс по соответствующему направлению.

В рамках направлений предусмотрено несколько уровней квалификации, а именно новичок, специалист, профессионал, эксперт и архитектор. Каждый уровень квалификации подтверждается соответствующим сертификатом Cisco.

Сетевая академия Cisco организована при Украинской академии банковского дела Национального банка Украины (УАБД НБУ) в городе Сумы. Ежегодно в ней проходят повышение квалификации сотрудники Национального банка Украины, а также проходят обучение студенты УАБД НБУ. Обучение осуществляется по направлению маршрутизация и коммутация. Сетевая академия оснащена всем необходимым оборудованием, которое используется слушателями для выполнения практических работ, связанных, прежде всего, настройкой и эксплуатацией

оборудования Cisco. Обучение в сетевой академии Cisco осуществляют сертифицированные инструктора из числа преподавателей УАБС НБУ, прошедших соответствующую теоретическую и практическую подготовку.

Поскольку спрос на специалистов, владеющих навыками настройки и эксплуатации оборудования Cisco, в банковском секторе растет, планируется увеличение номенклатуры направлений курсов Cisco и увеличение групп слушателей сетевой академии Cisco УАБД НБУ.

О.В. Кантаєва, *канд. екон. наук,* ***І.М. Боярко,*** *канд. екон. наук,*
ДВНЗ "Українська академія банківської справи НБУ"

СВІТОВІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ РИНКІВ СЕК'ЮРИТИЗАЦІЇ В КОНТЕКСТІ ЕКОНОМІЧНОГО РОЗВИТКУ ДЕРЖАВИ В УМОВАХ ГЛОБАЛЬНОЇ ФІНАНСОВОЇ КРИЗИ

Виникнення кризових явищ в діяльності банківських установ тісно пов'язано з відсутністю чітких уявлень про безпечність інформації, яка використовується для прийняття управлінських рішень як самим менеджментом банку, так і зовнішніми та внутрішніми контрагентами.

Захист інформації від всього можливого спектру потенційних загроз для безперервності підприємницької діяльності та зниження ефективності її проведення, з метою досягнення максимальної реалізації бізнес-можливостей щодо отримання та збереження доходів, становить сутність поняття "інформаційна безпека".

Для правильного розуміння змісту інформаційної безпеки необхідно враховувати, що термін "загрози" (threat) має декілька альтернативних визначень, закріплених в міжнародних нормативно-правових актах. Так, за визначенням, що надається Асоціацією аудиту та контролю інформаційних систем (ISACA), загроза – це будь-яка ситуація або подія, яка має потенційну можливість зашкодити системі. Згідно з Європейськими критеріями оцінки безпеки інформаційних технологій (European ITSEC), це – дія або подія, яка може поставити під сумнів безпеку.

Необхідно зазначити, що виникнення інформаційної безпеки слід пов'язувати, насамперед, з усуненням явища уразливості (Vulnerability). Дане поняття характеризує особливість інформаційних ресурсів, які можуть експлуатуватися загрозою та порушити загальну безпеку системи.

На нашу думку, забезпечення ефективного управління безпекою банку вимагає обов'язкового врахування вимог інформаційної

захищеності від загроз протиправного та несанкціонованого використання внутрішньої фінансово-аналітичної інформації, стратегічних та оперативних показників діяльності.

Сучасним інструментом стратегічного планування, який дозволяє збалансувати стратегічні та оперативно-тактичні цілі управління, інтегрувати відповідні завдання та функції, узгодити інтереси власників та менеджменту, є система збалансованих показників (Balanced Scorecard – BSC). Вона надає можливість адекватно оцінювати критичні фактори не лише поточного, але й майбутнього стратегічного розвитку банківських установ. Використання BSC забезпечує скоординоване управління такими процесами, як трансформація загального попереднього уявлення про можливості розвитку в цілеспрямовану стратегію, доведення її до всіх рівнів організаційної системи управління, обґрунтоване планування короткострокових параметрів розвитку банківської діяльності та поточний контролінг виконання планових цілей та завдань. Тобто в збалансованій системі показників міститься вся інформація, що відображає поточний стан та перспективи розвитку банку, а це зумовлює посилення вимог щодо її захисту та інформаційної безпеки.

Склад системи збалансованих показників, що використовуються банком в процесі управління його діяльністю, має бути підпорядкований загальній меті підвищення рівня фінансової безпеки банківської установи. При цьому загальний алгоритм формування такої системи передбачає: визначення джерел небезпеки та інформаційної бази для оцінки рівня їх впливу; класифікацію джерел за функціональними складовими загальної безпеки банку; відбір показників та їх групування за функціональними складовими загальної безпеки банку; визначення граничних значень показників та допустимих інтервалів їх змін з врахуванням характеру дії джерела небезпеки та ймовірності його прояву (ризику).

Оскільки процес стратегічного та оперативно-тактичного планування в банківських установах, як правило, є автоматизованим та передбачає використання мережевих технологій збору, систематизації, обробки та передавання даних, то важливою складовою створення умов для інформаційної безпеки систем управління, побудованих на збалансованих показниках, є обмеження доступу неавторизованих користувачів до такої інформації. Відповідно, формування правил такого обмеження зумовлює необхідність попередньої класифікації як самих показників, так і різних етапів їх використання в процесі розробки та реалізації стратегії розвитку банку за рівнями доступу та правами користувачів на здійснення тих чи інших операцій в інформаційній системі банку.

Визначення, досягнення, підтримка та вдосконалення інформаційної безпеки завжди є суттєвою складовою процесів підтримки конкурентоспроможності готівкового обігу, рентабельності, комерційної репутації, дотримання вимог нормативно-законодавчої бази, що регламентує підприємницьку діяльність в цілому та банківську зокрема.

М.В. Потанина, *ст. преподаватель*
кафедры менеджмента и экономико-математических методов
Севастопольского национального технического университета

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ РАЗДЕЛА, ПОСВЯЩЕННОГО ЗАЩИТЕ БИЗНЕСА, В РАМКАХ УЧЕБНОЙ ДИСЦИПЛИНЫ “ЭЛЕКТРОННАЯ КОММЕРЦИЯ”

Цель учебного курса Электронная коммерция – дать студентам экономических специальностей базовую подготовку по технологиям электронной коммерции и навыки по применению данных технологий. Студенты, успешно выполнившие учебный план, должны иметь представление об электронной коммерции, ее предметной области и методах осуществления; иметь опыт использования электронных систем взаиморасчетов, автоматизированных систем управления ресурсами предприятий, интернет-магазинов; иметь опыт работы в электронных аукционах и биржах, создания собственных коммерческих интернет-проектов. Особое место в данном курсе занимает направление, посвященное вопросам безопасности и защите бизнеса в рамках электронной коммерции.

Одним из важнейших условий широкого применения Интернета в электронном бизнесе было и остается обеспечение адекватного уровня безопасности для всех транзакций, проводимых через него. Это касается информации, передаваемой между пользователями, информации сохраняемой в базах данных торговых систем, информации, сопровождающей финансовые транзакции.

Понятие безопасность ведения бизнеса и, в общем, понятие безопасности передаваемой информации можно определить как состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Поскольку Сеть полностью открыта для внешнего доступа, то роль этих методов очень велика.

В рамках учебного курса Электронная коммерция рассматриваются ряд разделов, посвященных этой проблеме. В первую очередь дается

понятие криптографии – науки об обеспечении безопасности данных. Криптография призвана решать задачи конфиденциальности, аутентификации и целостности информации. В соответствии с названными задачами основными методами обеспечения безопасности выступают шифрование, цифровая подпись и сертификаты. Наиболее распространенными механизмами, призванными решить поставленные задачи и обеспечить безопасность проведения электронных платежей через Интернет сегодня являются:

- протокол SSL (Secure Socket Layer), обеспечивающий шифрование передаваемых через Интернет данных;
- стандарт SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

В рамках курса также изучается темы, посвященные уязвимостям и основным угрозам безопасности, видам мошенничества в электронном бизнесе и способам предотвращения их. Рассматриваются законодательные акты, определяющие государственное регулирование Электронной коммерции на Украине, и меры ответственности за нарушение существующего законодательства.

Таким образом, в заключении следует отметить, что, не смотря на все имеющиеся сложности, проблема обеспечения безопасности и защиты бизнеса на Украине является актуальной, а знания, даваемые по этому вопросу в рамках учебной дисциплины Электронная коммерция – востребованными.

В.В. Коваленко, *здобувач*
Національного університету державної податкової служби України;
Є.І. Марко, *старший науковий співробітник*
Військового інституту Київського національного університету
імені Тараса Шевченка

ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ (КОМУНІКАЦІЙНІ) ТЕХНОЛОГІЇ ЯК ВИЗНАЧАЛЬНИЙ ІНСТРУМЕНТ МІНІМІЗАЦІЇ РИЗИКІВ У ФІНАНСОВО-КРЕДИТНІЙ СФЕРІ

Інформаційно-комп'ютерні (комунікаційні) технології (ІКТ) усе більшою мірою стають фактором, що зумовлює системні й цивілізаційні зміни в глобальному вимірі.

Відіграючи багатогранну функціональну (пізнавально-освітню, інтеграційно-координаційну, інноваційно-модернізаційну, контрольно-безпекову і т.ін.) роль, ІКТ в той же час безпосередньо впливають на мінімізацію ризиків у фінансово-кредитній сфері.

За оцінкою фахівців Вищої школи бізнес-інформатики (м. Москва) вклад ІКТ в зростання ВВП розвинутих країн далекого зарубіжжя на початку XXI ст. складав від 20 до 40 %, при цьому ІКТ визначають 70–80 % у позитивній динаміці сукупної факторної продуктивності.[1] Дані показники з часом будуть значно вагомішими, оскільки в країнах, що включились у цивілізаційні перегони, ІКТ дозволяють оптимізувати взаємовідносини з постачальниками, планувати реальні виробничі завдання, ефективно управляти затратами на персонал, контролювати прозорість товарних та фінансових потоків і, в кінцевому підсумку, суттєво мінімізувати ризики, які неминуче супроводжують зазначені процеси.

Сфера інформаційних технологій (ІТ-сфера) в Україні перебуває у стані активного становлення. Загальний обсяг доходів, отриманих в ІТ-ринку у 2010 році, склав майже 21 млрд. грн. Найбільша частка доходів припадає на реалізацію засобів обчислювальної техніки та обладнання 80,4 %. Розробка програмного забезпечення становить 15,4 %, консультування з питань інформатизації – 1,4 %, оброблення даних – 1,0 %, ремонт і технічне обслуговування офісної та електронно-обчислювальної техніки – 1,7 %. На додаток до цього активно розвиваються такі послуги, як адаптування пакетів програм до специфічних потреб користувача, ІТ-аутсорсинг, створення та ведення баз даних тощо.

Найвищими темпами зростають доходи від послуг з розроблення програмного забезпечення та консультування у цій сфері (69 %), які в загальному обсязі наданих ІТ-послуг у сфері інформатизації складають майже 78 % всього обсягу провайдерських послуг. При цьому у зазначеному сегменті ринку працюють понад 2,9 тис. підприємств. Разом з тим, офіційний експорт програмного забезпечення за даними Держкомстату складає лише 0,1 % від загального обсягу доходів, отриманих від діяльності, пов’язаної з розробкою програмного забезпечення (ПЗ). З урахуванням “тіньової складової” загальний обсяг українського сегменту ринку, пов’язаного з розробкою програмного забезпечення, оцінюється в 2,6–3,5 млрд. грн. Тобто, від 15 до 37 % ринку з розроблення ПЗ знаходиться в тіні. Дана статистична інформація переконливо демонструє необхідність посилення фінансово-правового управління даними процесами.

Базовим сегментом у фінансово-кредитній сфері виступають банки. Лідером і модератором застосування сучасних інформаційно-комунікаційних технологій на теренах України, безумовно, є Національний банк. Саме державний центральний банк півтора десятиліття тому запровадив

[1] Див.: Вопросы экономики. – 2009. – № 10. – С. 91.

модульну систему (SAP-систему) на основі загальної ІКТ-аріхтектури, яка була покликана забезпечити єдиний інформаційний простір у рамках єдиної інформаційної програмної системи.

Головною стратегічною метою вопровадження SAP-систем було створення єдиного безпечного інформаційного простору, який дає змогу реалізувати загальний стандартний набір моделей операцій і поцесів, що функціонують в режимі реального часу, для фінансового, матеріального й управлінського обліку і, таким чином, для мінімізації ризиків у фінансово-кредитній сфері.

Необхідність і можливість створити інтерфейси з різними локальними програмними комплексами, але здатними до консолідації і подальшого інтегрального використання систематизованої інформації, стала суттєвою та відмітною ознакою вирішення проблеми створення єдиного інформаційного простору у фінансово-кредитній (банківській) сфері. НБУ за короткий період часу тричі оновлював ландшафт SAP-систем. При цьому корінна модифікація ІКТ здійснювалася в уовах діючої банківської системи, без порушення її функціонування і при дотримання жорстких вимог щодо безпеки. "Такого унікального гетерогенного апгрейду SAP-систем ніхто не проводив".[2]

Керівництвом НБУ розглядається також можливість інтеграції систем управління золотовалютними запасами Findur з Головною книгою FI в SAP ERP, а також інформаційне забезпечення банківських операцій з цінними паперами у національній валюті тощо. Наведений приклад переконливо демонструє конкретні кроки на шляху формування єдиного інформаційного простору у досить важливому сегменті національної економіки, яким є банківська система.

Ситуація з формуванням єдиного інформаційного поля у фінансово-креджитній сфері могла б бути значно кращою, якби виконавча влада країни практично реалізувала низку організаційно-управлінських та нормативно-правових заходів, передбачених Верховною Радою України, котра у свій час (13.08.99) схвалила "Концепцію науково-технічного та інноваційного розвитку України", а тодішній Глава держави видав Указ "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет". За умови практичної реалізації згаданої Концепції можна було б запровадити досить дієві механізми мінімізації фінансових ризиків і, таким чином, уникнути руйнівної банківської кризи 1998 р.

На часі виділити спеціальну бюджетну строку, яка б передбачала назріле фінансування розвитку сучасних Інтернет технологій в країні.

[2] Вісник Національного банку України. Науково-практичний журнал. – 2010. – № 8. – С. 11.

Не менш актуальною є розробка Національної програм Інтернет-інформатизації на 2010–2015 роки. У рамках даної Програми необхідно було б передбачити: розробку спеціального проекту на створення інформаційно-аналітичної системи, де б вагоме місце зайняв найбільш перспективний напрямок формування найсучаснішої системи Інтернеткомунікацій.

Як стверджують знані фахівці, інформаційне реагування через мережі Інтернет нині важливіше, аніж застосування якихось інших (а тим паче, традиційних) маркетингових комунікацій.[3] Навпаки, опора на традиційні комунікативні інструменти та засоби означатиме гарантоване безнадійне відставання, фіксація такої національної економіки у в'язкому болоті глобальної периферії.

InterNet є універсальним й максимально демократичним комунікаційним простором, у якому поліфонічно співіснують дуже різні цінності й інтереси, завдяки чому кількість учасників, що користуються ним, інтенсивно зростає. Інтернет, розкриваючи двері у віртуальну економіку, водночас зламує технологічні бар'єри, революційним чином посилює інноваційні можливості кожного окремого національного господарства. Переваги швидкісних Інтернет комунікацій усе більш активно й широко використовуються в фінансових операціях.

Перераховувати наочні і досить вагомі переваги застосування сучасних Інтернет технологій інформаційно досить об'ємно. Адже це своєрідний Всесвіт, перетворений в інформаційну форму, пересаджений у віртуальну реальність і компактно укладений в сучасні ІКТ.

Останнім часом у фінансово-кредитному сегменті мережі Інтернет активізувалися атаки на сайти та сервери банківських установ, а також спроби несанкціонованого отримання персональної інформації користувачів систем дистанційного банківського обслуговування (паролі, секретні ключі засобів шифрування, ПІН-коди і номера банківських карт, персональні дані клієнтів та аналогів їх власноручного підпису). Найбільш розповсюдженим видом хакерських впливів є так звані DOS-атаки або "відмова в обслуговуванні".

Для цього використовується така технологія. Велика кількість комп'ютерів (від декількох сотень і більше), програмне забезпечення яких попередньо спеціальним чином дистанційно модифікується, за командою хакерів починають одночасно направляти масові запити на відповідний ресурс (сайти та сервери), серйозно порушуючи або повністю блокуючи його роботу. При цьому власник сайту чи серверу, як правило, не в змозі самостійно, без допомоги провайдера Інтернету відновити працездатність ресурсу. Тривалість атак може продовжува-

[3] Див.: П.Р.Смит. Маркетинговые коммуникации. Комплесный поход. Перевод с английского. – К.: Знание-Пресс, 2003. – 25.

тися упродовж декількох діб. Такі дії фактично унеможливлюють дистанційне банківське обслуговування великої кількості клієнтів банку. Це призводить до прямих збитків, а також наносить великої шкоди престижу й авторитету відповідної банківської установи.

Виходячи з цього, доцільно рекомендувати фінансово-кредитним організаціям (банкам) включати в договори з провайдерами Інтернету зобов'язання сторін (з конкретними формами юридичної відповідальності) щодо недопущення "нештатних ситуацій" або ж про прийняття запобіжних заходів, спрямованих на оперативне відновлення роботи ресурсу.

Іншими різновидами хакерських атак є такі дії, спрямовані на неправомірне отримання персональної інформації користувачів системи дистанційного банківського обслуговування. Клієнтам по електронній пошті направляються повідомлення, в яких під дуже подібним на правду приводом (скажімо, йде звірка чи оновлення певного блоку даних банку) пропонується увести з клавіатури комп'ютера вказані коди (наприклад, через створений дублікат її web-сайта) у відповідне інформаційне поле. Водночас на комп'ютер клієнта з web-сайта можуть ретранслюватися заражені шкідливіми вірусами чи "закладками" програми, що дозволяють здійснювати приховані функції, націлені на отримання персональної інформації користувачів системи дистанційного банківського обслуговування.

Мають місце непоодинокі випадки неправомірного отримання реквізитів банківських карток при здійснення фінансових операцій через банкомати. При цьому використовуються накладні пристрої на клавіатуру для вводу ПІН-коду чи на пристрій для прийому карток в банкомат, а також спеціально пристосовані для таких цілей "фальшиві" банкомати, які зовнішньо не відрізняються від банкоматів, що застосовуються для дистанційного банківського обслуговування. Не є рідкістю також "телефонні махінації" та ін. форми злочинної діяльності у сфері Інтернет-технологій.

У ринково розвинутих країнах усе більшою мірою використовують "смарт-картки", які вміщують інтегральну мікросхему, тобто чіп-модулі з мікроконтролером, постійною пам'яттю і з можливістю перезапису. Запаяний у картку мікропроцесор, а по суті, мікрокомп'ютер дозволяє застосовувати різні програми, які залежать від інноваційного рівня маркетологів фінансової установи. Як результат, поки що не зафіксовано жодного випадку шахрайства з смарт-картками.

Це дає поштовх для подальшої інтернетизації небанківських платіжних операцій. У минулому році платіжна система Paupal (одна з найпопулярніших платіжних платформ у світі, що обслуговує левову

частку транзакцій у такій гігантській торговельній системі, як eBau) розпочала активно залучати до своїх інформаційних технологій розробників інших прогресивних систем, завдяки чому відбулася масова інтеграція у веб-сайти, мобільні програми й обладнання. Paupal – інтерфейс, надстроєний над пластиковою карткою, який дозволяє не повідомляти номер кредитної картки при здійсненні платежу у мережі Інтернет. Нині Paupal покриває біля 10 % глобальної Інтернет-комерції.[4]

В Україні, на жаль смарт-картки поки що не розповсюджені. Використовуючи цю ситуацію, мисливці за незаконним здобутком для перехоплення платіжних даних користувачів використовують такий різновид електронних вірусних махінацій, як маскування сайта під відому платіжну систему, які сприяють перехопленню даних щодо можливих грошових операцій та трансакцій, тобто "кейлоггер". За даними Національного банку України, кількість шахрайських операцій з використанням традиційних платіжних карток, випущених українськими банками, у 2009 році підвищилася у порівнянні з 2008 роком у 6,5 разів. У нинішньому році тенденція до зростання "електронного шахрайства" є досить чіткою.[5]

Виходячи з цього, Центральний банк держави (НБУ) має невідкладно розробити так звані "попереджувальні рекомендації", які мають сприяти зменшенню ризиків при банківському обслуговуванні клієнтів, зокрема при застосуванні систем Інтернет-банкінга. На часі офіційне продукування таких документів: "Щодо інформаційного змісту та організації web-сайтів грошово-кредитних організацій в мережі Інтернет"; "Про потенційні ризики при дистанційному банківському обслуговуванні"; "Рекомендації по організації управління ризиками, що виникають при здійсненні банками та ін. кредитними організаціями операцій із застосуванням систем Інтернет-банкінга".

Використання Internet (а також Intranet та Extranet) спільно з іншими новітніми інформаційними технологіями роблять віртуальну економіку прибутковою, а отже, і комерційно привабливою. Поза створенням й ефективним застосуванням сучасного інформаційного ринку і, зокрема, Інтернет-технологій, усе більшою мірою жодна країна не в змозі будувати й реалізовувати стратегію на максимальну мінімізацію фінансових ризиків.

Водночас в Україні склалася надзвичайна ситуація щодо управління адресним простором українського сегмента Інтернет, який понад десятиріччя здійснюється за межами державного кордону нерезидентами.

---

[4] Бочарський К. Небанківські платіжні системи на ринку фінансових мікротранзакцій / К.Бочарський // Фінансовий ринок України. – 2010. – № 8. – С. 16.

[5] Фінансовий ринок України. – 2010. – № 5. – С. 35.

У 2010–2015 рр. у рамках Національної програми важливо передбачити: впровадження реєстру національних електронних інформаційних ресурсів; розвиток системи інтегрованого доступу до інформації з мережі Інтернет та створення необхідної інноваційної бази ІКТ, що, зокрема, посилить регулятивні можливості держави і завдяки цьому відчутно мінімізує ризики у фінансово-кредитній сфері країни.

С.О. Шамов, *доц. кафедри інформаційних технологій*
Харківського інституту банківської справи Університету банківської справи НБУ

КОНТРОЛЬ ЯКОСТІ КЕРІВНИХ ДОКУМЕНТІВ ЯК НЕОБХІДНА СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙНИХ СИСТЕМ

Для ефективної протидії злочинній діяльності і забезпечення економічної безпеки країни в цілому велике значення має якість керівних документів: положень, інструкцій, настанов, описів процедур тощо, які регламентують діяльність посадових осіб, як елементів організаційної системи. Наявність упущень, протиріч, нестиковок в таких документах, їх системна неузгодженість створюють, з одного боку, умови для помилкових дій цих осіб, та, з іншого боку, умови для здійснення економічних злочинів. Це негативно впливає на стійкість системи та її здатність задовольняти потреби надсистеми (держави, суспільства). Оскільки всі керівні документи складені природною людською мовою, семантика і прагматика якої вкрай важко піддається комп'ютерній обробці, та мають у більшості випадків обсяг, що значно перевищує фізіологічні та інтелектуальні можливості людини, контроль їх якості з метою виявлення і виправлення названих недоліків є складною проблемою, що досі не знайшла свого задовільного розв'язання. Гострота актуальність цієї проблеми і те, що багаторічні зусилля науковців не призвели до розробки ефективних повністю формальних методів і комп'ютерних засобів автоматичного її розв'язання, змушують шукати ефективні рішення на шляху поєднання можливостей неформального природного інтелекту людини та формального штучного інтелекту комп'ютера.

Виходячи з того, що згадані вище керівні документи містять описи процесів функціонування складових організаційних систем або окремих їх аспектів, були проведені дослідження можливостей виділення людиною в тексті документу фрагментів, що описують окремі елементи процесу, їх поєднання у формальний опис процесу з подальшим контролем коректності отриманого опису відповідно до встановлених

формальних правил. Окремі аспекти цих досліджень представлені в літературі [1–3]. Об'єктами досліджень були обрані три групи керівних документів різного призначення, різних галузей і різних рівнів управління організаційними системами. До кожної з них була застосована однакова схема дослідження, яка складалась з наступних кроків:

1) визначення формальної алгебри, що використовувалась для аналізу коректності документів, та формальних вимог, яким повинні відповідати описи процесів у цій алгебрі;
2) розмітка тексту документів з метою виявлення і позначення фрагментів, що представляють структурні складові описуваних процесів, їх атрибутів, властивостей та характеристик;
3) відображення сукупності виділених фрагментів у формальну систему, підпорядковану заданій формальній алгебрі;
4) контроль відповідності формальної системи визначеним вимогам та реєстрація формального змісту виявлених невідповідностей;
5) відображення виявлених невідповідностей у сукупності текстових фрагментів, що були отримані на 2-му кроці;
6) змістовна інтерпретація невідповідностей, аналіз причин їх виникнення, можливих наслідків та шляхів усунення.

Але в межах цієї схеми виконані дослідження мали істотні відмінності. По-перше, вони різнились обраним формальним апаратом. В першому випадку була розроблена спеціальна алгебра продукційного типу, що враховувала особливості описуваних об'єктів. В другому і третьому випадках застосовувались формалізми мов структурно-функціонального моделювання сімейства IDEF [4]. По-друге, були застосовані різні способи контролю відповідності. В першому випадку були розроблені і застосовані відповідні інструментальні програмні засоби. В другому випадку застосовувались два варіанта контролю: візуальний та програмними засобами, що підтримують нотації IDEF. В третьому випадку контроль здійснювався без застосування програмних засобів.

Отримані результати засвідчили наступне:

1) формалізми, що були застосовані, дозволяють відобразити процеси функціонування організаційних систем, що описані в керівних документах різного призначення, галузей і рівнів управління;
2) ці формалізми придатні для відображення і виявлення неповноти, протиріч, нестиковок в таких документах, а також їх системної неузгодженості;
3) застосовані способи контролю відповідності документів встановленим формальним вимогам виявилися результативними у всіх трьох випадках;

4) якість документів розглянутих трьох груп виявилася досить низькою: мали місце всі види некоректності, що могли бути визначені у межах використаних формалізмів, середня щільність виявлених недоліків склала від 2 на сторінку у першій групі до 20 на сторінку у другій групі;
5) підхід, що був застосований для контролю якості документів, є результативним у всіх трьох випадках.

Таким чином, отримані результати підтвердили необхідність контролю і підвищення якості керівних документів для забезпечення економічної безпеки організаційних систем, а також свідчать про можливість і результативність застосування для цього описаного підходу.

Література

1. Шамов С. А. Средства формализации и контроля технических заданий на разработку программных систем. В сб. Повышение качества программных средств вычислительной техники. Тезисы докладов III Международной научно-технической конференции "Программное обеспечение ЭВМ", ноябрь 1990 г. – Тверь, Центрпрограммсистем, 1990 г.
2. Шамов С. О. Контроль коректності описів бізнес-процесів як складова аудиту інформаційних технологій. // Інформаційні технології в обліку та аудиті. Аудит інформаційних технологій: Збірник матеріалів Міжнар. наук.-практ. конф. 24–25 листоп. 2006 р. – Харків: ВД "Фактор", 2006. – С. 129–138.
3. Шамов С. О. Контроль описів банківських продуктів на основі структурно-функціонального моделювання. // Соціально-економічні проблеми сучасного періоду України. Фінансовий ринок України: глобалізація та євроінтеграція (Збірник наукових праць) / НАН України. Ін-т регіональнтх досліджень. – Львів, 2008. – Вип. 1 (69). – С. 431–438.
4. Дубейковский В.И. Эффективное моделирование с AllFusion Process Modeler 4.1.4 и AllFusion PM. – М.: ДИАЛОГ-МИФИ. 2007. – 382 с.

І.Л. Близнюк, *начальник відділу*
лабораторії проблем правового забезпечення діяльності ОВС
Державного науково-дослідного інституту МВС України"

ОСНОВНІ ЗАСАДИ ПОЛІТИКИ БЕЗПЕКИ БАНКУ

Політика безпеки банку – одно або декілька правил, процедур, практичних прийомів та керівних принципів з організації безпеки, якими керується банк у своїй діяльності.

Як правило, політика безпеки розробляється банком у вигляді окремого документа (положення), який затверджується правлінням банку. Виконання вимог зазначеного документа має забезпечуватися і контролюватися керівництвом банку та іншими відповідальними за його безпеку особами.

Перед розробкою політики безпеки співробітникам банку необхідно: мати чітке уявлення про моделі загроз і порушників, ідентифікувати активи, що підлягають захисту (так звані об'єкти захисту в банку),

та оцінити ризики ураження об'єктів банку. При цьому, розробляючи політику безпеки банку, необхідно обов'язково враховувати, як інтереси вкладників, так і особливості й інтереси конкретних власників банку, а також відносини як у колективі, так і між колективом і власниками або менеджментом банку, який представляє інтереси власників.

Ефективна політика безпеки банку має на увазі встановлення чіткого розподілу відповідальності банківських працівників на кожному етапі підготовки, оброблення та виконання електронних банківських документів на всіх рівнях.

Чинне банківське законодавство передбачає необхідність розробки та затвердження у банках таких основних адміністративно-розпорядчих документів, які безпосередньо пов'язані з питаннями забезпечення безпеки банку та впровадженням його ефективної політики безпеки:

- "Порядок використання і зберігання засобів захисту у банку в разі виникнення надзвичайних ситуацій", зокрема, внутрішній документ банку, який регламентує порядок відновлення роботи в системі електронних платежів Національного банку України (СЕП) у разі порушення роботи в системі або виникнення надзвичайних ситуацій (якщо банк – учасник СЕП). З цією метою банк має також забезпечити формування і зберігання архівів електронних банківських документів, а також надійне резервування для підтримки безперебійного функціонування внутрішньобанківської платіжної системи (ВПС);
- внутрішній документ, який регламентує порядок здійснення фінансового моніторингу банківських операцій, які можуть підпадати під ознаки легалізації (відмивання) доходів, одержаних злочинним шляхом;
- "Положення про порядок перевезення валютних цінностей та інкасації коштів банку";
- "Інструкція про порядок приймання під охорону (зняття з-під охорони) банку";
- "Порядок здійснення заходів та контролю з технічного захисту інформації у банку";
- "Інструкція, яка регламентує правила зберігання, захисту та використання інформації, що становить банківську, комерційну таємницю, та конфіденційної інформації";
- "Внутрішній порядок зберігання таємних ключів та інструкція із забезпечення безпеки експлуатації засобів криптографічного захисту інформації (КЗІ) в банку" (у процесі провадження банком криптографічного захисту інформації);
- "Правила системи переказу коштів" (якщо банк створив або є учасником міжнародної (або внутрішньобанківської, чи міжфілійної) платіжної системи.

У банку мають бути визначені строки, порядок зберігання та утилізації інформації з обмеженим доступом, а також вестись журнали реєстрації доступу до інформації з обмеженим доступом та засобів її обробки.

На сьогоднішній день в Україні достатньою мірою нормативно врегульовано процес організації діловодства з питань захисту інформації. Зокрема, у вітчизняних нормативно-правових актах зазначається, що діловодство з питань захисту інформації електронних банківських документів у банку ведуть (у випадку участі банку в СЕП): адміністратор захисту інформації; адміністратор АРМ-СЕП/АРМ-НБУ.

Крім того, у банку мають бути визначені функціональні обов'язки відповідальних осіб із захисту інформації.

Усі особи, відповідальні за роботу із засобами захисту інформації, мають бути призначені тільки згідно з розпорядчим документом банку.

Усі особи, які використовують у процесі роботи засоби захисту інформації, повинні підписати зобов'язання з належного їх використання.

У національних нормативних актах прописана процедура забезпечення безпеки банку в умовах таких нестандартних ситуацій: вихід з ладу апаратури криптографічного захисту інформації, якою він забезпечений завдяки НБУ; псування гнучкого магнітного диску (ГМД) з копією програмного модуля генерації ключів (ПМГК) або втрата ПМГК (та/або його копії) чи втрата контролю за місцезнаходженням ПМГК та/або його копії (у разі криптографічного захисту інформації); псування ГМД з таємними ключами (ТК), компрометація ТК або втрата контролю за ТК (у разі криптографічного захисту інформації); нестандартна ситуація в роботі інформаційної мережі, електронної пошти, в депозитарії та в системі "клієнт банку – банк", яка виникла внаслідок помилок, порушень з боку клієнтів та самих банків. Зокрема, національним законодавством визначений порядок використання і зберігання засобів захисту в банку в разі виникнення зазначених надзвичайних ситуацій.

Також нормативно-правовими актами України передбачені вимоги щодо технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, в яких є відомості з грифом "Банківська таємниця", та інша електронна інформація, доступ до якої обмежений банком, зокрема вимоги до систем електроживлення та заземлення, мережевого обладнання, приміщень з обмеженим доступом, комутаційних кімнат (приміщень, у яких розміщене телекомунікаційне устаткування, що забезпечує функціонування локальних і корпоративних мереж банку, а також зв'язок з іншими установами та мережами загального користування), серверних приміщень, приміщень, у яких зберігаються електронні архіви.

Крім того, у банку доцільно розробити такий документ з безпеки, як "Політика інформаційної безпеки банку".

Політика інформаційної безпеки банку створюється на основі результатів аудиту інформаційної інфраструктури та наявних систем і засобів захисту інформації банку.

Політика інформаційної безпеки повинна бути затверджена, видана та належним чином доведена до відома всіх співробітників банку. Політика повинна визначати відповідальність керівництва та викладати підхід банку до управління захистом інформації.

Доцільність розробки та затвердження такого документа передбачена міжнародними стандартами, зокрема, ISO 17799 "Інформаційна технологія. Практичні правила управління інформаційною безпекою".

Цей документ повинен містити такі положення:

- визначення інформаційної безпеки, її загальних цілей та сфери дії;
- виклад цілей та принципів інформаційної безпеки;
- короткий виклад найбільш істотних для банку політик безпеки, принципів, правил та вимог, наприклад:
  1) відповідність законодавчим вимогам та договірним зобов'язанням;
  2) вимоги відносно навчання питанням безпеки;
  3) запобігання появам та виявлення вірусів й іншого шкідливого програмного забезпечення;
  4) управління безперервністю функціонування банку;
  5) відповідальність за порушення політики безпеки;
- визначення загальних та конкретних обов'язків співробітників у межах управління інформаційною безпекою, включаючи інформування про інциденти порушення інформаційної безпеки;
- посилання на документи, які доповнюють політику інформаційної безпеки, наприклад, більш детальні політики та процедури безпеки для конкретних інформаційних систем, а також правила безпеки, яких повинні додержуватися співробітники банку на автоматизованих робочих місцях.

За стандартом ISO 17799 у банку має бути призначена відповідальна за політику інформаційної безпеки службова особа, яка повинна відповідати за її реалізацію та перегляд відповідно до встановленої процедури.

У положеннях стандарту ISO 17799, як у національних нормативно-правових актах, підкреслюється важливість використання цифрових підписів і шифрування для забезпечення конфіденційності переданої інформації між банками і т.п.; забезпечення безпеки інтернет-банкінгу; забезпечення стійкості до вірусних атак; забезпечення безпеки електронної пошти.

При цьому стандартом ISO 17799 вимагається, щоб криптографічні ключі, які використовуються для цифрових підписів, відрізнялися від тих, які використовуються для шифрування.

При використанні цифрових підписів необхідно враховувати вимоги національного чинного законодавства, яке визначає умови, при яких цифровий підпис має юридичну силу.

Отже, як національні нормативно-правові акти, так і міжнародні стандарти дозволяють розробити внутрішньобанківські документи із забезпечення безпеки банку, зокрема Положення про політику безпеки банку. Проте вказані міжнародні стандарти визначають вимоги до розробки лише тих документів банку, які безпосередньо стосуються питань захисту інформації на об'єктах інформаційних технологій. Але для розробки ефективної політики банку також мають бути розроблені адміністративні (режимні, організаційні) заходи безпеки як окремий напрям (вид) захисту банку, заходи щодо захисту інформації від витоку технічними каналами. Тому у цих питаннях необхідно користуватися національними стандартами (ДСТУ, нормативними документами НД ТЗІ), нормативними актами НБУ тощо.

Література

1. Міжнародний стандарт ISO 17799:2000 "Інформаційна технологія. Практичні правила управління інформаційною безпекою" ("Information technology – Code of practice for information security management").
2. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджені Постановою Правління НБУ від 02.04.2007 № 112.
3. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем, затверджене Постановою Правління НБУ від 25.09.2007 № 348.
4. Інструкція з організації охорони установ банків Державною службою охорони при Міністерстві внутрішніх справ України, затверджена Наказом МВС України від 23.08.2005 № 700.
5. Інструкція про міжбанківський переказ коштів в Україні в національній валюті, затверджена Постановою Правління НБУ від 16.08.2006 № 320.
6. Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України, затверджена Постановою Правління НБУ від 17.06.2004 № 265.

М.С. Удовик, *канд. юрид. наук, ст. науковий співробітник,*
доц. кафедри економіко-правових дисциплін
Національної академії внутрішніх справ

ДО ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДІЯЛЬНОСТІ БАНКУ

Організована злочинність активно і наполегливо намагається проникнути до найбільш прибуткових сфер діяльності комерційних структур. Тому проникнення до комерційних банків є особливо бажаною метою злочинних угруповань, адже підпорядкування їх злочинцям може дати великі можливості для здійснення значних махінацій, відмивання

“брудних грошей”, переведення їх за кордон та інших дій, які приносили б злочинним елементам величезні доходи.

Водночас умови конкурентної боротьби роблять нерівномірним розвиток підприємницької діяльності, у тому числі й у банківській сфері. Це, у свою чергу, створює необхідність постійного пошуку шляхів удосконалення виробництва і технологій та зберігання їх у таємниці. Пошук ринків, боротьба за клієнтів і нейтралізація конкурентів вимагають усебічної інформації. За таких умов ефективна діяльність банку може бути реалізована вжиттям як пасивних заходів безпеки, пов’язаних із різними видами захисту, так і активних дій сил безпеки, насамперед спрямованих на створення сприятливого інформаційного простору для роботи банку.

Забезпечення інформаційної безпеки банку передбачає виконання таких завдань:

- інформаційно-аналітичний супровід прийняття рішень керівництвом банку;
- протидія спробам несанкціонованого збору інформації з обмеженим доступом, яка є власністю банку, його клієнтів або партнерів.

Інформаційно-аналітичний супровід прийняття рішень керівництвом банку здійснюється шляхом збирання і аналітичної обробки інформації про стан і можливі перспективи діяльності суб’єктів банківського ринку. Метою цієї діяльності є виключення можливості несподіваної появи несприятливих факторів і загроз діяльності банку та забезпечення прийняття управлінських рішень, здатних мінімізувати наслідки негативного впливу сфери діяльності банку. Для досягнення цієї мети підрозділ безпеки використовує у своїй діяльності елементи комерційної розвідки, об’єктами якої є конкуруючі структури, а також юридичні і фізичні особи, які можуть бути або є клієнтами банку.

Джерелами інформації для комерційної розвідки банку є працівники відповідних установ, організацій, підприємств, банків, інші категорії громадян, які з тих чи інших причин мають доступ до відповідної інформації, засоби масової інформації, рекламні продукти, матеріали наукових досліджень, виробничі зразки тощо.

Основними сферами інформаційної уваги комерційної розвідки банку є:

- сфера інтересів – інформація про об’єкти, регіони, галузі економіки, до яких прагне проникнути банк у майбутньому, події, які характеризують відповідні ринки і банківський ринок в цілому;
- сфера впливу – інформація про події і об’єкти, що можуть здійснювати вплив на поточну діяльність банку;
- сфера безпосередньої діяльності – інформація про об’єкти та події, які характеризують або впливають на проведення поточних операцій банку.

Основними завданнями підрозділу безпеки з питань комерційної розвідки є:

- формування спеціальних інформаційних ресурсів банку;
- створення інтегрованих інформаційних баз даних;
- інформаційно-аналітичне дослідження об'єктів сфери інформаційної уваги банку;
- організація та проведення інформаційного моніторингу;
- розроблення інформаційних документів для забезпечення управлінських рішень керівництва банку;
- інформаційно-аналітичне дослідження клієнтів, партнерів, конкурентів та інформаційно-аналітичне забезпечення операцій і угод банку;
- аналіз ефективності технологій банківських операцій і послуг;
- розроблення пропозицій з удосконалення форм і методів діяльності підрозділів банку та перспектив їх розвитку.

Протидія спробам несанкціонованого збору інформації з обмеженим доступом у банку передбачає виконання заходів з попередження неправомірного отримання інформації банку спецслужбами, конкурентами та зловмисниками з використанням технічних засобів або через працівників банку.

Заходи протидії несанкціонованому збору інформації у банку спрямовуються на:

- розроблення відповідної нормативної бази, яка регулює режим і порядок доступу, зберігання і використання інформації банку;
- контроль дотримання заходів інформаційної безпеки працівниками банку;
- захист інформації в засобах і мережах її передавання та обробки.

Захист інформації банку з обмеженим доступом здійснюється усім персоналом банку відповідно до службових обов'язків.

Розроблення нормативної бази захисту інформації в банку і контроль дотримання інформаційної безпеки працівниками банку здійснює підрозділ безпеки.

Заходи захисту інформації в засобах і мережах її передавання та обробки передбачають використання апаратних, програмних та криптографічних засобів захисту.

Апаратні засоби захисту застосовуються для вирішення таких завдань:

- перешкоджання візуальному спостереженню і дистанційному підслуховуванню;
- нейтралізація паразитних електромагнітних випромінювань і наводок;

- виявлення технічних засобів підслуховування і магнітного запису, несанкціоновано використовуваних у приміщеннях банку;
- захист інформації, що передається засобами зв'язку і міститься в системах автоматизованої обробки даних.

Програмні засоби захисту представляють собою спеціальні програми, включені до складу програмного забезпечення комп'ютерів та інформаційних систем, які реалізують функції захисту конфіденційної інформації від неправомірних дій – несанкціонованого доступу, копіювання або руйнування.

Для захисту від несанкціонованого доступу за допомогою програмних засобів здійснюється:

- ідентифікація об'єктів і суб'єктів;
- розмежування доступу до інформаційних ресурсів;
- контроль і реєстрація дій з інформацією і програмами.

Захист інформації від копіювання забезпечується виконанням таких функцій:

- ідентифікація середовища, з якого запускається програма копіювання;
- аутентифікація середовища, із якого запущена програма копіювання;
- реакція на запуск із несанкціонованого середовища;
- реєстрація санкціонованого копіювання;
- протидія вивченню алгоритмів роботи системи.

Заходи захисту від руйнування інформації передбачають заборону використання у банку несанкціонованого програмного забезпечення, використання спеціальних антивірусних програм, виконання архівації і резервування інформації тощо.

Таким чином, забезпечення інформаційної безпеки банку – це система заходів із забезпечення необхідного рівня інформованості керівництва і персоналу банку, а також зовнішнього середовища, ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз, що досягається організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу в банку, аналітичною обробкою інформації; організацією системи інформаційного забезпечення прийняття рішень керівництвом банку; визначенням категорій банківської інформації та виробленням відповідних заходів її захисту; дотриманням відповідних режимів діяльності банку; виконанням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів витоку інформації та їх нейтралізації.

Є.М. Бодюл, *канд. юрид. наук,*
начальник відділу з організації науково-дослідної роботи
Національної академії внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ

Політика інформаційної безпеки банківської установи являє собою науково обґрунтовану систему поглядів на визначення основних напрямків, умов і порядку практичного рішення задач інформаційного захисту банківської справи від протиправних дій.

Під інформаційною безпекою банку розуміється стан захищеності інформації щодо власників, керівництва, клієнтів банку, технологій та інформаційних ресурсів банку від внутрішніх і зовнішніх погроз.

Забезпечення інформаційної безпеки є невід'ємною складовою частиною діяльності комерційного банку.

Стан інформаційної безпеки банку являє собою уміння і здатність банку протистояти будь-яким спробам завдати шкоди законним інтересам банку.

Об'єктами безпеки є:

- інформація про персонал (керівництво, відповідальні виконавці, співробітники);
- інформація щодо технологій, які використовуються банком;
- інформаційні ресурси (інформація з обмеженим доступом, що складає банківську та комерційну таємницю, інша конфіденційна інформація, надана у виді документів і масивів незалежно від форми і виду їхнього представлення), в тому числі:
- інформація щодо діяльності та фінансового стану клієнта, що стала відома банку у процесі обслуговування;
- інформація щодо всіх операцій банку та фінансова звітність банку.
- конфіденційні електронні мережі банку.

Конфіденційні електронні мережі банку – це сукупність електронного устаткування, допоміжного і спеціального обладнання та програмних засобів, призначених для обробки, передачі та зберігання інформації щодо всіх операцій банку та фінансової звітності банку, встановлених в операційних підрозділах банку, серверних, в інших місцях, а також конфіденційної інформації банку та клієнтів банку.

До відомостей, що становлять банківську та комерційну таємницю банку відноситься інформація, втрата якої здатна завдати шкоди інтересам банку або його клієнтів. Відомості по рахунках, вкладах та операціях клієнтів та кореспондентів у відповідності до вимог ст. 60 Закону України "Про банки та банківську діяльність становлять БАНКІВСЬКУ

ТАЄМНИЦЮ БАНКУ. Відомості з питань технології банківської діяльності, управління, фінансів та інших заходів банку, розголошення (передача, витік) яких може завдати шкоди інтересам банку, становлять КОМЕРЦІЙНУ ТАЄМНИЦЮ БАНКУ:

- відомості, втрата яких може привести до тяжких наслідків для фінансово-економічної діяльності банку чи його банкрутства, присвоюється гриф таємності "ЦІЛКОМ КОНФІДЕНЦІЙНО" (ЦК).
- відомості, втрата яких може нанести значних збитків конкурентно спроможності банку та його операційним актам, присвоюється гриф таємності "КОНФІДЕНЦІЙНО" (К);
- інші відомості з питань технологічної банківської діяльності, управління фінансів та інших доходів Банку становлять комерційну таємницю без присвоєння грифу таємності.

Політика визначає мету і задачі системи інформаційної безпеки, принципи її організації, функціонування і правові основи, види погроз безпеки і ресурси, що підлягають захисту, а також основні напрямки розробки системи безпеки, організаційний й інженерно-технічний захист.

Мета і задачі системи інформаційної безпеки.

Головною метою системи інформаційної безпеки є забезпечення стійкого функціонування банку і запобігання погроз його безпеці, захист від протиправних посягань, розголошення, утрати, витоку, перекручування і знищення службової інформації, порушення роботи технічних засобів, забезпечення виробничої діяльності, включаючи і засоби інформатизації.

Задачами системи інформаційної безпеки є:

- віднесення інформації до категорії обмеженого доступу (банківській і комерційній таємницям);
- протидія витоку такої інформації;
- віднесення КЕМБ до найбільш небезпечного об'єкту для витоку інформації і з цієї точки зору приділення їй додаткової уваги;
- прогнозування, своєчасне виявлення й усунення погроз інформаційній безпеці банку; причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушенню нормального функціонування і розвитку банку;
- створення механізму й умов оперативного реагування на погрози інформаційній безпеці банку;
- ефективне припинення посягань на інформаційні ресурси банку на основі правових, організаційних і інженерно-технічних мір і засобів забезпечення безпеки.

Принципи організації і функціонування системи інформаційної безпеки банку.

Організація і функціонування системи інформаційної безпеки банку повинна відповідати наступним принципам: комплексність, своєчасність, безперервність, активність, законність, обґрунтованість, спеціалізація, взаємодія і координація, удосконалювання, централізація управління, економічна доцільність і порівнянність можливого збитку і витрат на забезпечення безпеки (критерій "ефективність – вартість").

Успішне й ефективне рішення задач забезпечення інформаційної безпеки банку досягається формуванням системи положень, правил, інструкцій, регламентів і функціональних обов'язків співробітників підрозділів і служб, у тому числі і Служби економічної безпеки. Необхідною умовою забезпечення інформаційної безпеки банку є сукупність правил входу (виходу) осіб у приміщення банку, внесення (виносу) документів, у тому числі і на з'ємних електронних носіях, правил збереження інформації, як на конкретному комп'ютері так і в комп'ютерній мережі.

Функціональні підрозділи виконують вимоги інформаційної безпеки банку. Керівники окремих підрозділів Банку несуть особисту відповідальність за дотриманням вимог інформаційної безпеки.

Література

1. Закон України "Про банки та банківську діяльність". № 2121-III від 07.12.2000 р.
2. Закон України "Про захист інформації в автоматизованих системах". № 80/94 від 05.07.94 р.
3. Указ Президента про " Положення про технічний захист інформації в Україні". № 1229/99 від 27.09.99 р.
4. Постанова КМ України про затвердження "Концепції технічного захисту інформації в Україні". № 1126 від 08.10.97 р.
5. Положення про вимоги щодо технічного стану та організації охорони приміщень банків України. Постанова Правління Національного банку України від 17 вересня 2003 року № 403. Зареєстровано в Міністерстві юстиції України 13 жовтня 2003 р. за № 925/8246.
6. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. № 423 від 11.10.96 р.
7. Закон України "Про інформацію". № 2657-XII від 02.10.92 р.
8. НД ТЗІ 1.1-004-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації комп'ютерних системах від несанкціонованого доступу.

І.Г. Андрущенко, *канд. юрид. наук,*
доц. кафедри економіко-правових дисциплін
Національної академії внутрішніх справ

СПІВВІДНОШЕННЯ РЕОРГАНІЗАЦІЇ ТА РЕСТРУКТУРИЗАЦІЇ ФІНАНСОВИХ УСТАНОВ

Реорганізація (франц. reorganisation – перетворення, від re... – префікс, що означає поновлення або повторення дії, і organisation – впорядкування, від лат. *organum* – інструмент, знаряддя) – перетворення або зміна структури чи організаційної форми установи, а також перебудова будь-якої системи чи структури управління. З огляду на юридичний зміст та наслідки, реорганізація означає припинення діяльності юридичної особи та виникнення нової з відповідним обсягом прав та обов'язків. В Україні законодавчо визначено п'ять форм реорганізації: поділ, злиття, виділення, приєднання і перетворення.

Реорганізація провадиться з дотриманням вимог антимонопольного законодавства за рішенням власника, а у випадках, передбачених чинним законодавством, – за рішенням власника та за участю трудового колективу або органу, уповноваженого утворювати такі установи, чи за рішенням органів суду. Реорганізація установи, що зловживає своїм монопольним становищем на ринку, може здійснюватися також шляхом її примусового поділу в порядку, передбаченому законодавством. Законодавством передбачено вирішення питань правонаступництва установ, що реорганізуються. Зокрема, у разі злиття установ усі майнові права та обов'язки кожної з них переходять до установи, що виникла в результаті злиття. При приєднанні однієї установи до іншої до останньої переходять усі майнові права та обов'язки приєднаної установи. У випадку поділу установи до нових установ, які виникли в результаті цього поділу, переходять за роздільним актом (балансом) у відповідних частинах майнові права та обов'язки реорганізованої установи. При виділенні з установи однієї чи кількох нових установ до кожної з них переходять за роздільним актом (балансом) у відповідних частинах майнові права та обов'язки установи, що реорганізується. У разі перетворення однієї установи на іншу до установи, яка щойно виникла, переходять усі майнові права та обов'язки колишньої установи. Установа вважається реорганізованою з моменту виключення її з державного реєстру [1, 292].

Аналізуючи реорганізацію як спосіб придбання бізнесу, слід торкнутися такого знакового терміну, що останніми роками набув досить широкого поширення, як – реструктуризація.

Реструктуризація (від лат. re... – префікс, що означає зворотну дію, і structura – побудова, розташування, порядок) – комплекс організаційно-господарських, фінансово-економічних, правових, технічних та інших

заходів, спрямованих на зміну структури установи, її управління, форми власності, організаційно-правової форми тощо, з метою фінансового оздоровлення установи, посилення її конкурентоспроможності, підвищення ефективності діяльності та інвестиційної привабливості. Здійснюється з метою поліпшення фінансового стану установи, запобігання її банкрутству, залучення вітчизняних та іноземних інвестицій.

Процедура реструктуризації, як правило, передбачає: прийняття компетентним органом або уповноваженою особою рішення про реструктуризацію суб'єкта господарювання; утворення спеціальної комісії, що здійснює контроль за проведенням реструктуризації; розроблення та впровадження відповідного проекту реструктуризації. Фінансування заходів з реструктуризації може здійснюватися за рахунок потенційних інвесторів, а також коштів установ, що реструктуризуються [1, 299].

Висловлюючись сократівською логікою, не всяка формально-правова реорганізація спричиняє реструктуризацію установи, але будь-яка глибока реструктуризація пов'язана із злиттям, приєднанням установи або перетворенням її організаційно-правової форми. Реорганізація відноситься більше до правової оболонки бізнесу, а реструктуризація – явище більш широкоформатне. Її предмет – бізнес у цілому як працююча система, що розвивається.

Актуальність проблеми реструктуризації фінансових установ обумовлена кількома причинами. Головні з них – перехід України до ринкової економічної системи, підвищення фінансових ризиків установ в умовах ринкової економіки, розвиток конкурентної боротьби між установами і групами компаній у різних сегментах ринку, боротьба за перерозподіл власності та глибока фінансово-економічна криза, що охопила вітчизняну економіку останніми роками.

Не дивлячись на популярність і поширене вживання терміну "реструктуризація" в засобах масової інформації та ділових колах, класичний правовий сенс цієї категорії залишається багато в чому незрозумілим. Нині законодавче (легальне) визначення "реструктуризація" фактично відсутнє.

Реструктуризація фінансової установи – крупна разова зміна у структурі капіталу чи власності компанії. Реструктуризація бізнесу полягає в корінній зміні системи ведення бізнесу, його структури. Це може бути зміна процесів бізнесу, відмова від деяких напрямів діяльності, зміна комерційної стратегії. Реструктуризація бізнесу може проводитися паралельно з реструктуризацією кредиту банківській установі (іноді – на її вимогу) або реструктуризацією боргу установи в цілому.

У цьому розумінні (та відповідному йому економіко-правовому явищі суспільного життя) можна виділити принаймні три основні чинники:

- фінансовий (перетворення структури активів і пасивів установи);
- структурний (перетворення внутрішньої структури та системи зовнішніх взаємозв'язків установи);
- організаційно-правовий (юридична процедура та технології реструктуризації установи, одним з яких є реорганізація).

Реструктуризацію установи можна позначити як сукупність правових процедур, направлених на перетворення її організаційної або власницької структури та (чи) оптимізацію структури активів і пасивів.

Підкреслимо, що якщо реорганізацію найчастіше використовують при дружньому поглинанні компанії-мети, то реструктуризація – один з основних превентивних оборонних заходів при організації корпоративної оборони від можливого недружнього корпоративного захоплення. Для слабо захищеного бізнесу властива консолідація власницьких, управлінських та операційних функцій в одній компанії, що спрощує завдання агресору. Щоб ефективно поглинути бізнес, йому потрібно здійснити перехоплення управління лише в одній компанії.

Одним з найефективніших превентивних заходів, направлених на захист установи від недружнього поглинання, є реструктуризація. В цілях захисту під реструктуризацією розуміється зміна внутрішньої структури бізнесу шляхом виділення відособлених підрозділів установи в незалежні юридичні особи, формальна зміна власників активів або їх диверсифікація, використання механізму перехресного володіння тощо.

Головним елементом реструктуризації є виділення власницького, виробничого, управлінського і торгового блоків діяльності установи, коли ці функції виконує не одна структура, а чотири самостійні юридичні особи (так звана схема чотирьох кутів). Власницька установа є володарем головних активів бізнесу і практично не бере участі у поточній господарській діяльності, що значно знижує ризик виникнення неконтрольованої кредиторської заборгованості, судових суперечок тощо.

Фінансові установи користуються активами на підставі договору оренди, але також закриті від зовнішнього середовища. Найбільш активну діяльність на ринку здійснює установа, яка відповідає за реалізацію на ринку фінансових послуг. Нарешті ядром схеми "чотирьох кутів" є керуюча установа, яка зосереджує професійних управлінців, фінансистів та юристів. Її основні функції – ведення бухгалтерського обліку всіх установ групи, правовий супровід, оптимізація фінансових потоків і загальна координація.

Основним власником акцій або часток участі у власницькій установі й інших юридичних особах найчастіше виступає некомерційне партнерство. До його складу входять основні власники бізнесу та один чи декілька можновладців з бізнес-еліти або ж органів влади. Здійснення такої реструктуризації дозволяє вирішити відразу декілька завдань: вивести із зони ризику основні активи бізнесу, оптимізувати фінансові потоки та забезпечити захист безпосередньо власників бізнесу [2, 141–142].

Література

1. Шемшученко Ю. С. Юридична енциклопедія : в 6 т. / Шемшученко Ю. С. – К. : Укр. енцикл. – 2003. – 5 т. – 733 с.
2. Орлов А. А. Покупка и продажа бизнеса. Российская практика / А. А. Орлов, С. А. Рибаков. – М. : Вершина, 2006. – 272 с.

С.М. Нужний, *канд. техн. наук,*
доц. кафедри ЕОС та ІБ ІАЕ
Національного університету кораблебудування імені адмірала Макарова

ЛАБОРАТОРНИЙ КОМПЛЕКС TIGRIS – 161 – 1М ДОСЛІДЖЕННЯ ПЕМВН ПЕОМ ДЛЯ ПІДГОТОВКИ СТУДЕНТІВ З ГАЛУЗІ ЗНАНЬ 1701 “ІНФОРМАЦІЙНА БЕЗПЕКА” ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ ПІДРОЗДІЛІВ ТЗІ

Входження України в світові економічні відносити на фоні повної відкритість її економіки для зовнішніх впливів та внутрішніх протиріччях призвело до стрімкого росту економічних злочинів і недобросовісної конкуренції. Одним із “нових” напрямків незаконного отримання інформації про діяльність конкурентів стало використання приладів, які дозволяють перехопити сигнали моніторів та відеокарт сучасних персональних електронно-обчислювальних машинах (ПЕОМ), на яких обробляється конфіденційна інформація.

Європі і Канаді використовується термін “compromising emanation” – компрометуюче випромінювання. В Америці використовують термін “TEMPEST”.

Історія виявлення ПЕМВН своїми коренями уходить в далекий 1918 рік, коли Герберт Ярдлі (Herbert Yardley) зі своєю командою був залучений військовими Силами США для дослідження методів виявлення, перехвату та аналізу сигналів військових телефонів і радіостанцій.

Термін побічне електромагнітне випромінювання і наводки (ПЕМВН) появився в кінці 60-х – на початку 70-х років.

До недавнішнього часу використання ПЕМІН було прерогативою спецслужб та розвідок. Основними перевагами цього напрямку

є використання “беззахідної” технології несанкціонованого доступу (НСД) до інформації з обмеженим доступом (ІзОД) та можливість отримувати сигнал із-за межі контрольованої зони.

В [1–3] проаналізовано можливість отримання зловмисниками НСД до ІзОД і визначено шляхи протидії. При цьому основний об’єм робіт припадає на проведення контрольних і профілактичних заходів, ефективність яких залежить від підготовленості персоналу служби технічного захисту інформації підприємства (фірми, організації та ін.).

Мета проекту: ознайомлення студентів та слухачів з теоретичними основами причин виникнення ПЕМВН в ПЕОМ та інших пристроях оргтехніки, здобуття практичних навичок роботи зі спеціалізованим обладнанням – апаратно-програмними комплексами.

Технічні вимоги до керуючої ПЕОМ:

- 32-х чи 64-х бітний процесор з тактовою частотою 2400 МГц та вище;
- ОЗУ 1024 Мб та більше;
- близько 600 Мб вільного простору на жорсткому диску;
- SVGA-відеокарта та монітор;
- ОС Windows 2000, XP, Vista, Windows 7;

Програмний засіб дає можливість проведення експрес-аналізу амплітудно-частотної характеристики випромінювання ПЕОМ на фоні природного фону та штучних перешкод, а також ідентифікувати обладнання, при роботі якого виникає ПЕМВН.

Найбільшу небезпеку, з точки зору витоку інформації, представляють побічні (паразитні) випромінювання технічних засобів, що беруть участь в процесі передачі, обробки і зберігання конфіденційної інформації. Основними каналами витоку інформації за рахунок ПЕМВН можуть бути:

- електромагнітні поля розсіювання технічних засобів;
- наявність зв’язків між інформаційними ланцюгами і різними струмопровідними лініями (система заземлення; мережа електроживлення; ланцюги зв’язку, які знаходяться в тому ж кабелі, що і інформаційні мережі; допоміжні технічні засоби і системи, що мають лінії зв’язку, розташовані в тих же приміщеннях; різні металеві трубопроводи; металоконструкції будівель і інші протяжні струмопровідні лінії).

Лабораторний стенд оснований на спеціалізованому приймальному пристрою – ресивері TIGRIS – 161 – 1M, який забезпечує виявлення та обробку сигналу з урахуванням впливу перешкод.

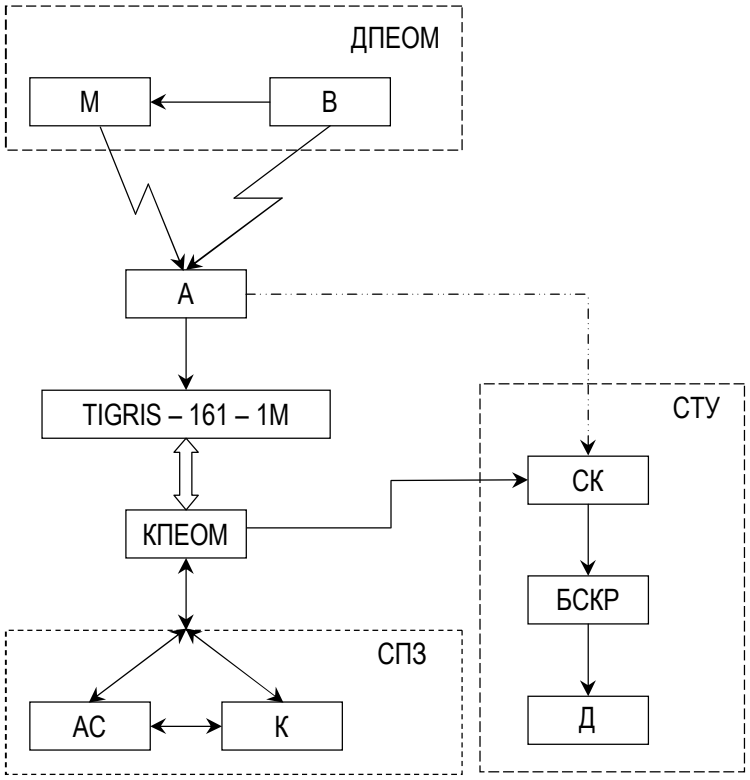


Рис. 1. Структурна схема лабораторного комплексу TIGRIS – 161 – 1М

ДПЕОМ – дослідна ПЕОМ до складу якої входять: В (відеокарта) та М (монітор); СТУ – спеціалізована телевізійна установка в складі: СК (селектор каналів), БСКР (блок рядкового та кадрового розгорнення; Д – дисплей); А – антенна; КПЕОМ – керуюча ПЕОМ з встановленим СПЗ (спеціалізованим програмним забезпечення) у складі: АС (аналізатор спектру) та К (корелятор).

Комплект з монітора, відеокабелю та відеокарти є найслабкішою ланкою в системі безпеки сучасних ПЕОМ. Для нормальної роботи електронно-променевої трубки потрібні високі рівні сигналів, внаслідок чого монітор є “найгучнішим” випромінюючим елементом.

Використання спеціалізованого програмного забезпечення дозволяє оперативно визначати параметри прийнятого сигналу та корегувати алгоритм обробки тест-сигналів з метою забезпечення кореляції.

Розробка таких алгоритмів дозволить своєчасно виявляти шпигунські програми, які встановлені на ПЕОМ з метою формування технічного каналу витоку конфіденційної інформації.

Розроблений лабораторних комплекс призначений для підвищення кваліфікаційного рівня спеціалістів, які випускаються університетом за напрямом підготовки 6.170102 “Системи технічного захисту інформації” (дисципліна “Захист інформації від витоку по технічним

каналам" та "Технічна експлуатація систем та пристроїв ТЗІ") і спеціалізації 6.170101 "Безпека інформаційних і комунікаційних систем" (дисципліна "Системи технічного захисту інформації") та 6.170103 "Управління інформаційною безпекою" (дисципліна "Системи технічного захисту інформації", "Захист інформації від витоку по технічним каналам").

Стан розробки: β-версія програмного забезпечення приймального пристрою ресивера TIGRIS–161–1M, розроблено програму та методику виконання лабораторних робіт.

Література

1. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. – К.: Нелк, 2001. – 139 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005. – 960 с.
3. Опарин В.В. Обнаружение средств съема речевой и видеоинформации. – Николаев: НТЦ "Квант", 2008.
4. Зайцев А.П., Шелупанов А., Мещеряков Р. и др. Техническая защита информации: Учебник для вузов. – М.: Горячая линия-Телеком, 2009. – 615 с.
5. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. 141 с.
6. Communications receiver ICOM IC-PCR1500. Service manual. – 2009. – 86 с.
7. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО "Издательство Машиностроение", 2009 – 508 с.
8. Нужний С.М, Андрійченко О.В., Кузьмін В.І. Скануючий спектральний корелятор для пошуку та аналізу джерел радіовипромінювання TIGRIS-161-1. – Вісник Східноукраїнського національного університету ім. В. Даля. Науковий журнал. – Луганськ, 2009, – № 6 (136).

О.А. Щелконогов, *ст. преподаватель ИАЭ*
Национального университета кораблестроения

СИСТЕМА КОНТРОЛЯ ВСКРЫТИЯ АППАРАТУРЫ ДЛЯ БАНКОВСКОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Использование системы контроля вскрытия аппаратуры (СКВА) имеет смысл при наиболее полном перекрытии всех каналов несанкционированного доступа, т.е. для вычислительных систем и сетей с повышенными требованиями к защите информации. Банковские сети относятся именно к таким объектам защиты. Поэтому разработанная система СКВА предлагается к использованию для защиты банковских компьютерных сетей.

СКВА предназначена для контроля доступа к внутреннему монтажу аппаратуры, технологическим пультам управления, кабельным соединителям, т.е. к таким элементам компьютерной сети, которые в

процессе эксплуатации при нормальном функционировании должны находиться в неизменном состоянии. Иначе это состояние называют механической целостностью системы.

Для обеспечения определенных гарантий того, что в данный момент в обработку информации не вмешиваются посторонние процессы, за исключением случайных, и служит контроль механической целостности аппаратуры [1].

Примеры реализации СКВА описаны в литературе [1, 165–177], [2, 359–360]. В имеющихся системах можно выделить следующие недостатки: недостаточная гибкость настройки и масштабирования, недостаточная защищенность от злоумышленника. В описываемой дальше системе сделана попытка устранить указанные недостатки.

СКВА состоит из трех основных элементов: датчиков вскрытия аппаратуры, цепи сбора сигналов и специального рабочего места централизованного контроля.

За основу всей системы предлагается использовать ПЭВМ и распределенную микропроцессорную систему с радиально-последовательным принципом построения управляющей сети. Такой принцип повышает стойкость всей системы к возможным повреждениям отдельных узлов, дает возможность реализации модульного программирования, а также уменьшает всю ее стоимость. Радиально-последовательный принцип удобен при использовании системы для рассредоточенных объектов (в отдельных комнатах на разных этажах с разной концентрацией оборудования).

Структурная схема показана на рис. 1.

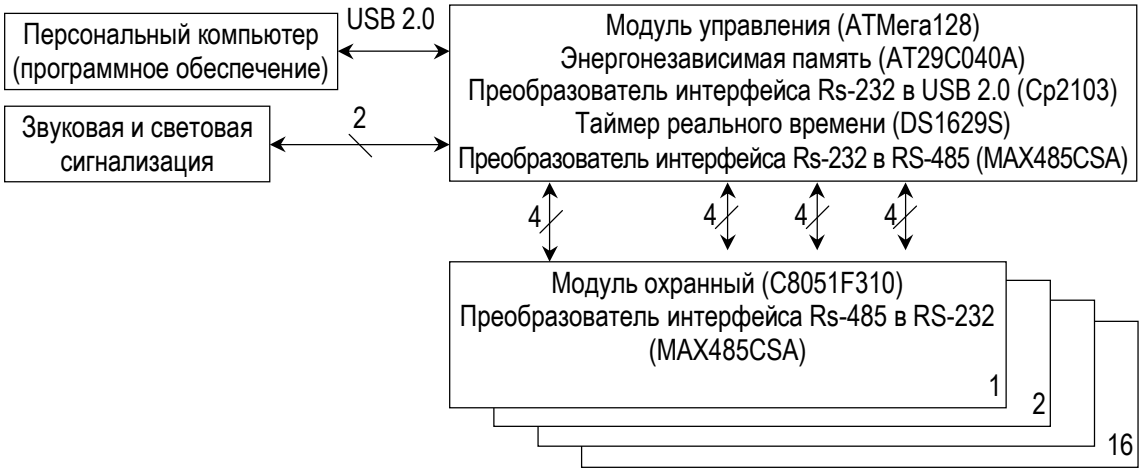


Рис. 1. Структурная схема системы СКВА

Данная микропроцессорная система позволяет контролировать положение 256 датчиков. Они соединены в 4 луча, по 4 модуля охраны в каждом луче и по 16 опрашиваемых датчиков в каждом модуле охраны.

ПЭВМ в системе обеспечивает интерфейс работы системы и оператора, отображая на экране дисплея всю информацию о положении контролируемых датчиков. Кроме этого оператор может управлять режимом работы отдельных датчиков.

ПЭВМ связано с Модулем Управления (МУ) по интерфейсу USB 2.0. Основная цель работы МУ – сбор информации о состоянии датчиков, которыми управляют Модули Охраны (МО). МУ может работать и без связи с ПЭВМ, накапливая информацию о времени срабатывания датчиков (таймер реального времени) в энергонезависимой памяти до следующего сеанса связи, но выдавая сигнал тревоги на сирену при срабатывании датчиков. МУ расположен в непосредственной близости к ПЭВМ, а МО распределены периферийно по объектам, в непосредственной близости с контролируемыми устройствами. Связь МУ и МО осуществляется по интерфейсу RS-485 (этот интерфейс рассчитан на передачу на достаточно большие расстояния и устойчив к помехам). Кроме этого МУ выполняет функцию электропитания всех МО.

Основой всего МУ является микроконтроллер фирмы Atmel ATMega 128. Он управляет всеми процессами МУ. На микроконтроллер приходят данные с ПЭВМ через интерфейс USB 2.0, которые конвертируются в стандартный для ATMega 128 интерфейс RS-232 (в ТТЛ уровнях). Микроконтроллер управляет коммутацией четырех каналов (лучей), с помощью схемы коммутации. В каналах проводится преобразование интерфейса RS-232 в RS-485. Через эти каналы все Модули Охраны обмениваются командами и данными с главным микроконтроллером. Временные данные, предназначенные для ведения журнала событий, главный микроконтроллер получает из микросхемы таймера реального времени. Информация, которую микропроцессор не смог передать на ПЭВМ, сохраняется в микросхеме долговременной памяти типа Flash. При необходимости эти данные можно повторно переслать позднее.

Основой МО является микроконтроллер фирмы Silabs C8051F310. Он управляет опросом датчиков. На микроконтроллер приходят данные с МУ по интерфейсу RS-485, которые преобразуются в интерфейс RS-232, стандартный для микроконтроллера. Микроконтроллер управляет опросом 16 герконовых датчиков. Датчики сгруппированы по 4 в 4 шлейфа. Состояние датчиков кодируется в пакет сообщения и отправляется назад на МУ.

В качестве датчиков выбраны управляемые магнитные контакты (герконы) по типу переключающего реле с тремя выводами (центральный, замыкающий и размыкающий). Герконовый контакт управляется магнитным полем (от миниатюрного магнита, устанавливаемого на крышке или дверце). Этот выбор обусловлен дешевизной герконов, стойкостью их к внешним помехам и простотой в использовании.

Также усложняется доступ злоумышленника, поскольку одна цепь размыкается, а другая одновременно замыкается при движении магнита. Центральный вывод реле подключается к аналого-цифровому преобразователю (АЦП), а два других к цепям питания через резисторы. Такое включение разрешает отслеживать положения геркона, проводить контроль на обрыв и замыкание трехпроводной линии связи к датчику. Использование АЦП повышает общий уровень защищенности, поскольку ведется контроль за разными уровнями сигнала, а не за наличием или отсутствием таких.

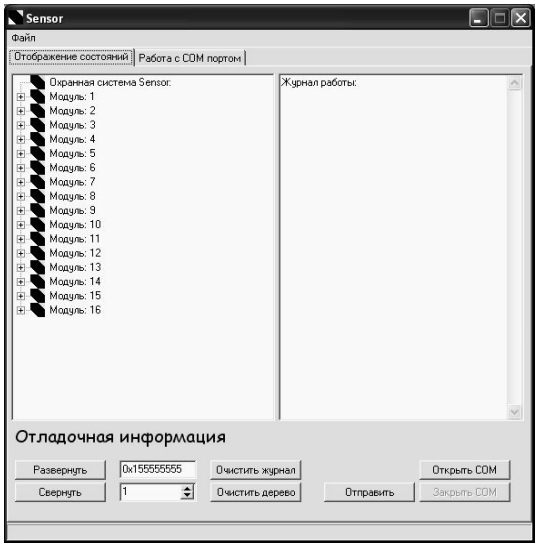
Программное обеспечение верхнего уровня (уровня ПЭВМ) разработано на языке С++. ПО включает следующие видовые формы:

- отображение состояния датчиков древовидным вложенным списком;
- ведение текстового журнала событий и происшествий с указанием даты и времени момента срабатывания датчика;
- настройка коммуникационных портов.

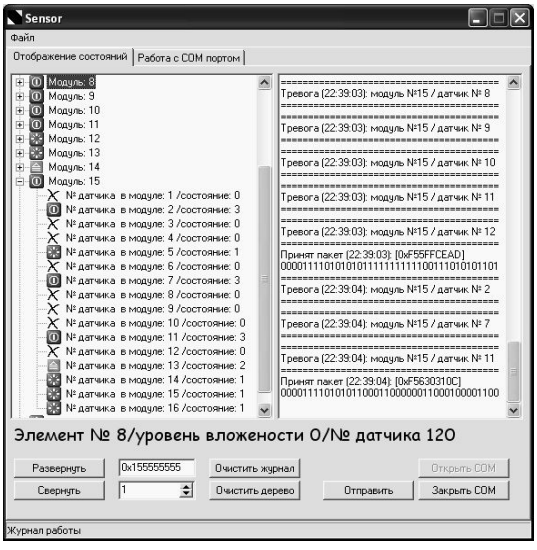
Ниже (рис. 2) приведены фрагменты рабочих режимов программного обеспечения.

В программе ведется временной журнал событий: принятая посылка и двоичное представление принятого кадра. Кроме того, в журнале отображается прием сигнала тревоги с указанием времени, модуля и датчика, на котором зафиксировано состояние тревоги.

Программа имеет интуитивно понятный и логически сгруппированный интерфейс. Подписи на функциональных кнопках дают информацию об их назначении, а дополнительная информация отображается в нижней строке состояния в виде подсказок.



Фрагмент А



Фрагмент Б

Рис. 2. Фрагменты рабочих режимов работы пользовательского программного обеспечения

Таким образом, данная система удовлетворяет всем основным требованиям, которые предъявляют к системам контроля раскрытия аппаратуры. Использование как рабочего места ПЭВМ позволяет интегрировать СКВА в банковскую компьютеризированную систему защиты информации.

Література

1. Мельников В.В. Защита информации в компьютерных системах. – Москва: Финансы и статистика, Электронинформ, 1997. – 364 с.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – Санкт-Петербург: Наука и Техника, 2004. – 384 с.

В.І. Сліпченко, *канд. юрид. наук,*
доц. кафедри кримінального процесу
Запорізького юридичного інституту ДДУВС

ЗАХИСТ БАНКІВСЬКОЇ ТАЄМНИЦІ ЯК СКЛАДОВА ПОЛІТИКИ БЕЗПЕКИ БАНКУ

Становлення України як правової держави вимагає реформування всіх сфер життя суспільства, і зокрема, правовідносин у економічній сфері. Як наслідок, на сьогодні постала необхідність удосконалення законодавства, що регулює банківський сектор економіки. Така необхідність пов'язана, перш за все, з усуненням прогалин у законодавстві, які призвели до затяжної фінансово-економічної кризи 2008 та 2009 років. По-друге – з необхідністю запровадження принципово нових систем захисту в автоматизованих системах інформації, що становить банківську таємницю або є конфіденційною.

Створення авторизованих систем, а відповідно, введення в дію нових продуктів (послуг) банківських установ ("SMS-банкінг", "Інтернет-банкінг", "WebMoney Banking" та ін.) дозволяє клієнтові управляти своїм рахунком навіть зі свого персонального комп'ютера чи мобільного телефону.

Не зважаючи на загальну доступність та простоту вказаних послуг, вони містять і відповідні елементи захисту: це спеціальна процедура реєстрації на сайті банку, запит логіна і пароля клієнта, а також отримання спеціального одноразового коду в банкоматі для зазначеного виду операції.

Слід також відзначити, що такий вид банківської інформації на підставі ст. 60 Закону України "Про банки і банківську діяльність" утворює банківську таємницю, що охороняється як кримінальним (ст. 232 КК України), так і цивільним законодавством (ст. 1076 ЦК України).

Зазначена обставина вимагає забезпечення належного рівня захисту інформації про клієнта та операцій на його рахунках, оскільки сам банк не є власником зазначеного виду таємниці, а виступає лише її утримувачем.

Постановою Національного банку України від 14 липня 2006 року № 267 затверджено Правила зберігання, захисту, використання та розкриття банківської таємниці (які зареєстровані в Міністерстві юстиції України 3 серпня 2006 року за № 935/12809). Зазначені правила є обов'язковими для всіх банківських установ та запроваджені з метою запобігання несанкціонованому доступу до інформації, що містить банківську таємницю. Працівники банку, які мають доступ до такої інформації, повинні встановлювати особливий порядок реєстрації, використання, зберігання та доступу до документів, що містять банківську таємницю. Контроль за дотриманням Правил покладено на НБУ.

За даними Департаменту зв'язків із громадськістю МВС України, в нашій державі кожного року зростає рівень кіберзлочинності у середньому на 16 %.

Із запровадженням такого виду послуг, як "SMS-банкінг", "Інтернет-банкінг", "WebMoney Banking", та постійним зростанням рівня кіберзлочинності в нашій державі з'являється реальна загроза навмисного перехоплення технічними засобами комп'ютерних даних, а саме інформації про клієнта та операції на його рахунках.

Враховуючи існування зазначеного виду банківських послуг, інформації, що може бути перехоплена за допомогою технічних пристроїв, та межі банківської таємниці, на нашу думку, доцільно виділити дві групи інформації, що становить інтерес для злочинців. До першої групи відноситься інформація про клієнта, а саме його персональні дані, які дозволяють ідентифікувати особу. Друга – інформація про рахунки клієнта та операції на них.

Зазначена обставина вимагає від банківських установ не лише декларування належного рівня інформаційної безпеки, але і вжиття конкретних засобів захисту інформації з обмеженим доступом.

У наукових та організаційних цілях політика безпеки банківської установи здійснюється за двома напрямами: внутрішній та зовнішній. Вони поділяються на охорону банківської та комерційної таємниці, інформаційну безпеку, кримінологічну та фізичну безпеку банку. Зазначені напрями безпеки є пов'язаними між собою.

У свою чергу, для з'ясування належного рівня організації політики безпеки банку, на нашу думку, доцільно застосувати такі критерії, як:

1) вид банківської операції;
2) вжиті організаційно-технічні форми та засоби захисту інформації.

Інформаційна безпека банку – це організація гарантованого захисту інформаційних ресурсів банку, відповідна професійна підготовка працівників у галузі інформаційних технологій, що забезпечує захист інформаційних ресурсів та інформаційних потоків від несанкціонованого доступу до них.

У зарубіжній літературі для характеристики рівня інформаційної безпеки традиційно застосовуються п'ять принципів: широта, глибина, централізація, контрольований доступ і персональний контроль.

На нашу думку, політика інформаційної безпеки банку, крім зазначених принципів, також повинна відображати філософію, стратегію та методи захисту інформації з обмеженим доступом.

Дня належного рівня протидії злочинності, її профілактики та захисту банківського сектору економіки держави від протиправних посягань необхідна допомога і правоохоронних органів, яка може надаватися наступним чином.

Правоохоронні органи за допомогою банківських установ повинні створювати та сприяти наповненню таких баз даних, як:

- картотека осіб, причетних до вчинення злочинів з використанням пластикових карток, фіктивних платіжних документів або підроблених банківських гарантій;
- картотека осіб, причетних до шахрайства з грошовими переказами в українському сегменті мережі Інтернет;
- картотека осіб, причетних до фіктивного підприємництва, шахрайства з фінансовими ресурсами або нецільового використання кредитів;
- картотека осіб, причетних до розголошення інформації, що становить банківську або комерційну таємницю.

У кожному випадку вчинення злочину в кредитно-фінансовому чи банківському секторі економіки правоохоронні органи повинні з'ясовувати та досліджувати: ступінь організованості суб'єктів злочину; спосіб його підготовки, вчинення та приховування; характеристику особи злочинця; причини та умови, які сприяли його вчиненню.

Зроблені аналітичні висновки (наприклад, за рік) необхідно доводити до відома Національного банку України та інших банківських установ з метою вжиття відповідних заходів реагування, усунення виявлених недоліків у роботі банківської системи та розробки контрзаходів.

Підсумовуючи, відзначимо, що увага правоохоронних органів до організації політики безпеки банку обґрунтовується тим, що банківський сектор є складовою економіки держави. Остання, в свою чергу, є невід'ємним елементом національної безпеки України.

О.О. Савченко, *доц. Донецького юридичного інституту*
Луганського державного університету внутрішніх справ імені Е.О. Дідоренка

ПРОТИДІЯ ЗАГРОЗАМ ФІНАНСОВОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ У СУЧАСНИХ УМОВАХ

Постанова проблеми. В умовах збільшення фінансового капіталу в економіці України, розвитку малого та середнього бізнесу, наявності кризових явищ у банківських державних та недержавних установ, рівень забезпечення економічної, і зокрема, фінансової безпеки не відповідає існуючим вимогам сьогодення, а тому стає актуальним питання щодо її забезпечення, участі в цьому правоохоронних органів, і в першу чергу, відповідних спеціальних підрозділів міністерства внутрішніх справ.

Вважаємо, що це питання необхідно розглядати комплексно. По-перше: з розкриття поняття фінансової безпеки та його складових, По-друге: з розгляду відповідних заходів щодо взаємодії між відомчими службами безпеки банківських установ та правоохоронними органами.

Розгляд проблеми. В сучасних умовах господарювання в Україні, діяльність банківських установ, незалежно від форм власності, є достатньо складним і ризикованим заняттям. І це пов’язано не тільки з далеко не найкращим загальним станом національної економіки, різними макроекономічними деформаціями, кризовими явищами, а з низкою специфічних факторів, що негативно впливають на економічну безпеку фінансових установ. На наш погляд і погляд науковців серед таких факторів найбільше значення мають такі:

- збереження високого рівня тінізації та криміналізації економіки взагалі, поширення злочинних дій з метою відмивання “брудних” грошей та вивозу їх за кордон;
- недосконаліть чинного законодавства, що регулює відносини у сфері фінансів;
- відсутність достатнього досвіду в організації, розробці та реалізації заходів захисту власної фінансової безпеки;
- недостатня кількість досвідчених фахівців-професіоналів з питань протидії фінансовим загрозам діяльності банківських установ;
- нізкий рівень взаємодії фінансових установ, їх служб безпеки з правоохоронними органами тощо [7, 54–63, 9, 104–105].

Відомо що, у процесі здійснення фінансової діяльності банки можуть стикатися з протиправними діями й відчувати негативний вплив з боку різних фізичних і юридичних осіб, що безпосередньо чи опосередковано спрямований на дестабілізацію фінансового стану банку.

У цьому зв'язку постає питання про поняття загроз їх фінансової безпеки, оскільки у кінцевому рахунку такі загрози виражаються в значних матеріальних та грошових втратах.

Враховуючи погляди науковців на це питання та на нашу думку, за джерелами виникнення існують внутрішні та зовнішні фінансові загрози.

Внутрішні загрози це такі: що пов'язані з недоліками та прорахунками у діяльності самого банка, які можуть призвести до негативних наслідків, а саме:

- низький рівень контролю за здійсненням фінансово-господарських операцій організації роботи з конфіденційними документами, які можуть бути об'єктами неправомірних зазіхань;
- неефективна робота внутрішній служби економічної безпеки;
- низький організаційний рівень захисту платіжних та комп'ютерних систем від підробки та несанкціонованого доступу.

До зовнішніх загроз відносять такі, джерела яких перебувають поза межами підприємства:

- промислове шпигунство, таємне спостереження за співробітниками фірми, зараження комп'ютерних програм вірусами, засилання копіювання комп'ютерних програм і даних, підслуховування переговорів тощо;
- незаконні дії конкурентів, доведення банку до банкрутства із використанням засобів масової інформації та розповсюдженням чуток серед населення та вкладників про збитковість банківської установи, її фінансової неспроможності виконати свої зобов'язання щодо виплат депозитів;
- викрадення комп'ютерної інформації шляхом незаконного втручання інших злочинів з використанням високих технологій, погрози фізичних розправ над співробітниками банку та їх близькими, пограбування і розбійні напади тощо [4, 32–41, 5, 13–19].

Вважаємо що організація, побудова та функціонування комплексної системи фінансової безпеки повинні ґрунтуватися на основі додержання таких основних принципів як: законність, компетентність, плановість, координація та взаємодія тощо.

На наш погляд, важливе місце в діяльності відомчої служби економічної та фінансової безпеки банківської установи повинен займати принцип постійної взаємодії з правоохоронними органами, й передусім, з державною службою боротьби з економічною злочинністю, недавно створеними в МВС України департаментами фінансової та економічної

безпеки, боротьби з кіберзлочинністю та торгівлею людьми, яка може здійснюватися у напрямах:

- кадрового забезпечення – перевірка правоохоронними органами кандидатів на роботу працівників служби економічної безпеки, керівництва філій банків;
- інформаційного забезпечення – взаємний обмін інформацією про факти та способи вчинення злочинних дій, потенційно небезпечних осіб;
- організаційно-технічному – передбачає створення системи спільної протидії злочинним проявам, в тому числі, пов'язаними з підробкою та протиправним використанням платіжних карток, фінансовим шахрайствам, кіберзлочинністю та ін.

Враховуючи, що банківські правовідносини і взаємозв'язки між суб'єктами банківського регулювання з питань фінансової безпеки мають важливу роль щодо формування економічної безпеки в цілому держави, слід зазначити, що гарантії економічної безпеки банківської системи надаються і правоохоронними органами, зокрема спеціальними підрозділами МВС України.

На нашу думку, до цього часу, незважаючи на певні зміни, які були зроблені зокрема, до Закону України "Про Національний банк України", деякі з них, ще мають декларативний характер, особливо в тій його частині, яка стосується здійснення банківського нагляду та взаємодії з отримання правоохоронними органами банківської інформації або інформації про злочинні посягання у цій сфері, про які стало цим установам відомо. Негативно на цю діяльність впливає і відсутність Закону України " Про приватну детективну та охоронну діяльність в Україні". В процесі дослідження нами було проведено опитування понад 50 співробітників банківських установ розташованих у м. Донецьку, яке показало що через небажання керівництва банків та фінансових установ зіпсувати свій імідж та недооцінку професіоналізму працівників правоохоронних органів (70 % опитуваних) керівництво не завжди зацікавлено взаємодії з правоохоронними органами [1; 3, с. 177].

На законодавчому рівні, на жаль, не передбачено порядок взаємодії банківських установ з правоохоронними органами у попередженні злочинів. Закон України "Про організаційно-правові основи боротьби з організованою злочинністю" не відображає необхідного оперативного механізму доступу до банківської інформації суб'єктів зловживань, бо чинне законодавство не передбачає ні якої відповідальності посадових осіб банків за ухилення від надання правоохоронним органам такої інформації. Існуюча практика отримання дозволу та отримання такої

інформації за допомогою суду спрацьовує тільки при певних умовах (існування кримінальної справи) [2, п. 4, ст. 17]. Щодо попередження злочинів, то це питання до цього часу не вирішене. Тому стає очевидною необхідність внесення пропозицій щодо вирішення цих питань. Вони можуть бути такими:

По-перше: треба внести певні зміни до адміністративного законодавства, які б передбачали відповідальність посадових осіб банківських установ за відсутність на їх підприємствах певних механізмів протидії злочинним посяганням, а також відсутності заходів щодо взаємодії у цих питаннях з правоохоронними органами.

По-друге: декриміналізації банківських установ сприяло б удосконалення системи банківського супроводжувального контролю. Безумовно, введення у дію певних змін до фінансово моніторингу дасть змогу вирішити окремі питання, але не в повному обсязі.

По-третє: треба налагодити та законодавче передбачити врегулювання взаємодії відомчих служб безпеки банківських установ з правоохоронними органами з питань попередження та розкриття злочинних посягань. На цей час існують різні посередницькі фірми, які пропонують свої послуги щодо повернення кредитів та ін. Нерідко вони використовують протиправні методи, порушують права людини. Тому вкрай необхідно прийняти Закон України “ Про приватну детективну та охоронну діяльність” [3, с. 178–179].

Можна з упевненістю стверджувати, що розглянуті питання треба вирішувати і комерційним банкам і державі, яка повинна створити такі організаційно-правові умови, які б сприяли найбільш ефективній роботі банківських установ.

Література

1. Закон України “ Про внесення змін до деяких законодавчих актів України щодо діяльності Національного банку України” // Голос України. – 2010. – № 133 – липень. 21.
2. Закон України “Про організаційно-правові основи боротьби з організованою злочинністю”// Відомості Верховної ради України. – 1993. – № 35.
3. Савченко О.О., Новикова Н.І., Рижков Е.В. Основи економічної безпеки та попередження злочинів у процесі інвестиційної діяльності банківських та фінансових установ: Науково-практичний посібник / За заг. ред. О.О. Савченка. – Донецьк: ТОВ “Юго-Восток ЛТД”, 2008. – 204 с.
4. Савченко О.О. Оперативно-розшукова профілактика й розкриття злочинів у сфері діяльності банківських і кредитно-фінансових установ. Курс лекцій: навчальний посібник. – Донецьк: ДЮІ, 2009. – 334 с.
5. Ніколаюк С.І., Никифорчук Д.Й. Безпека суб’єктів підприємницької діяльності: Курс лекцій / Серія: Бібліотека оперативного працівника. – К.: КНТ, 2005. – 320 с.

6. Чернявський С.С. Злочини у сфері банківського кредитування (проблеми розслідування та попередження): Навч. посібник / За заг. Ред. О.М. Джужи. – К.: Юрінком Інтер, 2003. – 264 с.
7. Кравчук С.Й. Економічна злочинність в Україні. Курс лекцій. Навчальний посібник. – К.: "Кондор", 2009. – 282 с.
8. Бутузов В.М., Павловський В.Д., Тітуніна К.В., Шеломенцев В.П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток. Науково-практичний посібник / За ред. І.В. Бондаренка. – К.: 2009. – 182 с.
9. С.В. Веліканов, А.Ф. Волобуєв, В.А. Журавель, С.С. Кисельова, І.М.Осика, Р.Л. Степанюк, В.М. Шевчук. Криміналістична профілактика економічних злочинів: Науково-практичний посібник / За ред. Д-ра юрид.наук, проф. В.А. Журавля). – Х.: "Харків юридичний", 2006. – 236 с.

Секція 2

МЕТОДОЛОГІЯ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРІВ, СИСТЕМ І КОМП'ЮТЕРНИХ МЕРЕЖ

А.М. Зима, *генерал-майор міліції,*
заступник Міністра внутрішніх справ України

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ У БАНКІВСЬКІЙ СФЕРІ: СТАН, ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Ми живемо в епоху інформаційного суспільства, коли інформаційні та телекомунікаційні технології охопили майже всі сфери життєдіяльності. Але людство, створивши безпрецедентний технічний проект – глобальну комп'ютерну мережу Інтернет, очевидно не могло передбачити, які можливості для зловживань створюють ці технології. Сьогодні жертвами злочинців, які вчиняють злочини у віртуальному просторі, можуть стати не тільки окремі люди чи юридичні особи, але й цілі відомства і навіть держави. При цьому безпека сотень тисяч людей може опинитися в залежності від кількох злочинців. Кількість злочинів, що вчиняють в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. Комп'ютерна кримінальна епідемія розвивається стрімкими темпами. За оцінками Інтерполу, швидкість зростання злочинності в глобальній мережі Інтернет, є найбільшою порівняно з іншими видами злочинів, включаючи торгівлю наркотиками та зброєю.

Світовий оборот злочинних угруповань від кіберзлочинів досягає 105 мільярдів доларів на рік. Майже 75 % користувачів Інтернету хоча б один раз в житті ставали жертвами кібернетичного злочину. При цьому майже 50 % постраждалих навіть не повідомляли поліцію про те, що стали жертвою комп'ютерних шахраїв, оскільки вважають, що віртуальних правопорушник-ків не вдасться притягнути до відповідальності.

Про масштаби злочинної діяльності говорять цифри, наведені на конференції Інтерполу, яка відбулась 15–17 вересня цього року в Гонконгу: викрадені кредитні картки продають на "чорному ринку" за ціною від 5 до 20 доларів. Досвідчений комп'ютерний шахрай "заробляє" в середньому 23 000 доларів на тиждень.

Кіберзлочинність не знає державних кордонів. Її транснаціональний характер породжує проблему кваліфікації злочинів, яка має

бути вирішена шляхом уніфікації національних законодавств. На це спрямована дія Міжнародної конвенції про кіберзлочинність, яка була укладена 23 листопада 2001 року в м. Будапешт і до якої нещодавно приєдналась Україна.

На думку фахівців, вчиненню Інтернет-злочинів мимоволі сприяють самі жертви – користувачі комп'ютерів, які проявляють зайву довірливість, нехтують елементарними правилами захисту конфіденційної інформації. Підвищена віктимність користувачів обумовлюється також ефектом "невидимості" злочинця, відсутністю будь-яких ознак його злочинних намірів.

За словами Генерального секретаря Інтерполу Рональда Ноубла, кібернетична злочинність вже ввійшла до переліку найбільш серйозних загроз з тих, з якими доводилося стикатися поліції. Міжнародне співтовариство перебуває сьогодні на етапі пошуку методів боротьби з цією проблемою, напрацювання єдиної політики з даного питання.

Небезпеку кіберзлочинності як для всього світу, так і для України усвідомлюють правоохоронні органи нашої держави. Вважаємо, що в Україні кіберзлочинність сьогодні є однією з найбільших загроз національній безпеці в інформаційній сфері.

Із застосуванням інформаційних технологій злочинці реалізують різного роду шахрайські схеми, здійснюють підробку грошових знаків, документів (в тому числі фінансових). Вони використовують електронні платіжні системи для "відмивання" коштів, здобутих злочинним шляхом. Кіберпростір використовується для незаконної торгівлі наркотиками, зброєю, розповсюдження дитячої порнографії, проведення різного роду екстремістської діяльності (зокрема, пропаганди насильства, жорстокості, расової, національної, релігійної нетерпимості), порушення авторських прав тощо. Окрему категорію становлять злочини, спрямовані проти нормального функціонування комп'ютерних систем та мереж: створення, розповсюдження та використання комп'ютерних вірусів, викрадення комп'ютерної інформації, хакерські атаки на комп'ютерні системи тощо.

За останні роки в Україні було виявлено 3 252 злочини, пов'язані із застосуванням інформаційних та телекомунікаційних технологій, з них розкрито 68,9 %, зокрема:

Рік	2005	2006	2007	2008	2009	Всього
Виявлено злочинів	615	583	656	691	707	3 532
те ж відносно 2005 р.	1	0,95	1,07	1,12	1,15	–
Розкрито злочинів	362	415	475	572	610	2 434
те ж у %	63,7	71,2	72,4	82,7	86,2	68,9

Отже, з року в рік можна спостерігати сталу тенденцію до зростання кількості кіберзлочинів в Україні. За останні п'ять років їх кількість зросла на 15 %. Разом з тим, близько 14 % таких злочинів сьогодні залишається нерозкритими.

Значну частину кіберзлочинів в Україні складають злочини у сфері банківської діяльності.

Сьогодні в Україні діє понад сотні банків, які використовують внутрішньодержавні й міжнародні карткові платіжні системи та здійснюють емісію і еквайринг платіжних карток. За даними спеціалістів щороку кількість операцій із застосуванням платіжних карток емітованих українськими банками значно збільшується, при цьому сума операцій складає більше 100 млрд. грн.

Аналіз криміногенної ситуації свідчить про зростання кількості злочинних проявів, коли об'єктом посягання або інструментом вчинення злочинів стають сучасні комп'ютерні та комунікаційні технології. Особливістю цих правопорушень є високий рівень технічного забезпечення злочинної діяльності, латентність, організованість, наявність розгалужених міжрегіональних та міжнародних зв'язків.

За останні п'ять років динаміка зростання злочинів у сфері комп'ютерних технологій становить приблизно 13–15 % щорічно, що відповідає існуючим тенденціям розвитку економічних показників та інформаційно-телекомунікаційної сфери в Україні.

Забезпечення правопорядку у сфері електронних платежів, комп'ютерних та Інтернет-технологій, а також на ринку телекомунікацій, виявлення та усунення причин та умов, що сприяють вчиненню цих злочинів поступово стає одним із пріоритетів в діяльності правоохоронних органів.

Моніторинг криміногенної ситуації у сфері комп'ютерних технологій свідчить, що найбільш поширеними видами злочинів у сфері функціонування електронних платежів є:

- підроблення платіжних карток та інших платіжних інструментів, збут підроблених карток, збут інформації про реквізити справжніх платіжних карток;
- шахрайське використання справжніх платіжних карток та їх підробок, у тому числі їх реквізитів у мережі Інтернет;
- несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж, з метою отримання інформації про реквізити справжніх платіжних карток.

Аналіз матеріалів за напрямом комп'ютерних та Інтернет технологій показав, що за останні три роки встановлено тенденцію до збільшення шахрайських дій в мережі Інтернет, в тому числі отримання персональної інформації (паролів, банківських рахунків або дампів

з інформацією про власників кредитних карт тощо), шляхом розсилки електронних листів від імені банку, які містять посилання на підроблені сайти, що імітують роботу справжніх – так званого "фішингу". В подальшому зазначена інформація використовується для ініціювання з-за кордону неналежних грошових переказів та поштових відправлень. Цьому сприяло стрімке розповсюдження Інтернет-аукціонів, "фінансових пірамід", використання небанківських електронно-платіжних систем.

Так, у Дніпропетровській області викрито групу осіб, які з використанням мережі Інтернет здійснювали втручання в роботу автоматизованої електронної системи Інтернет-магазину "Webmoney.ua", через який здійснюється реалізація різноманітних товарів, приймаючи в якості оплати платіжні картки міжнародних платіжних систем та облікові фінансові одиниці небанківських платіжних систем (Webmoney, E-gold, Ukrmoney), тим самим порушивши порядок обробки інформації у ній. У ході проведення заходів було встановлено, що зловмисники, використовуючи віддалене з'єднання з автоматизованою системою Інтернет-магазину "Webmoney.ua", шляхом несанкціонованої зміни інформації, сформували 58 підроблених платіжних доручень, за якими з електронного гаманця зазначеного магазину перерахували на свій електронний гаманець понад 1 млн. гривень. Відносно зловмисників СУ ГУМВС України в Дніпропетровській області порушено кримінальну справу за ч. 3 ст. 190 та ч. 1 ст. 361 КК України.

Усі злочини у сфері комп'ютерних технологій характеризуються загальними рисами:

- високим рівнем латентності, який обумовлений, зокрема, феноменом невизнанням провайдерами інтернет-послуг, банками, операторами зв'язку існування проблем несанкціонованого доступу до баз даних, викрадення паролів тощо, бо така інформація впливає на їх імідж, конкурентоспроможність тощо;
- використанням, при вчиненні злочинів, новітніх технологій, найсучаснішого апаратного та програмного комп'ютерного забезпечення; при недостатній теоретичній та практичній підготовці працівників регіональних підрозділів ОВС, нерозуміння ними технічних деталей та можливих схем вчинення високотехнологічних злочинів;
- організованістю, міжрегіональними та міжнародними зв'язками, вчинення злочинів з використанням інформаційних ресурсів, які територіально розміщені у різних країнах, що ускладнює проведення як оперативних, так і процесуальних заходів (наприклад, "карткові" злочини вчиняються організованими групами, діяльність яких має міжнародний характер (зв'язки злочинців, місця отримання та використання інформації про справжні платіжні картки, міжнародний характер розслідування тощо).

Міністерством внутрішніх справ України вжито низку організаційних та практичних заходів з метою забезпечення ефективної протидії злочинності у сфері інформаційних технологій. Можна виділити наступні напрями:

Перший – законодавче забезпечення боротьби з комп'ютерними злочинами, створення необхідної нормативно-правової бази.

З метою надання офіційного статусу взаємодії підрозділів між країнами СНД підписана та діє Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 1 червня 2001 р.

З метою правового забезпечення боротьби зі злочинністю у сфері високих технологій, МВС спільно з іншими зацікавленими відомствами утворено міжвідомчу Робочу групу з аналізу законодавства у сфері протидії і запобігання махінаціям з банківськими кредитними картками, іншим фінансовим злочинам, пов'язаним з комп'ютерними технологіями. До складу Робочої групи увійшли також представники СБУ, Національного банку України, Державної Судової адміністрації, Держфінмоніторингу, Державної податкової адміністрації України.

Членами Робочої групи розроблено та подано на розгляд і Верховної Ради України ряд законопроектів у сфері протидії "картковій" злочинності та комп'ютерній злочинності. За результатами цієї роботи Верховною Радою України прийнято Закони України "Про ратифікацію Конвенції про кіберзлочинність", "Про внесення змін до Кримінального та Кримінально-процесуального кодексів України" (щодо відповідальності за комп'ютерні злочини); Закону України "Про внесення змін до деяких законів України (щодо управління ризиками, вимог безпеки до здійснення операцій з платіжними картками та іншими платіжними інструментами та покарання за злочини з їх використанням)".

Департаментом ДСБЕЗ підписаний з Українською міжбанківською асоціацією членів платіжних систем ЄМА "Порядок надання інформації про сумнівні операції з використанням платіжних карток", яким забезпечується доступ до найсвіжішої інформації про факти вчинення правопорушень.

Порядком також передбачено, що за зверненням працівників ДСБЕЗ, спеціалісти Асоціації, у межах компетенції, сприяють забезпеченню наступних заходів:

- дослідження платіжних карток щодо їх відповідності стандартам, встановленим міжнародними платіжними системами;
- надання пояснень у якості спеціалістів щодо процедур карткових розрахунків та надання методичної допомоги правоохоронним органам з питань виявлення "карткових" злочинів;

- участь у якості спеціалістів при документуванні “карткових” правопорушень;
- навчання працівників правоохоронних органів, які безпосередньо займаються розкриттям та розслідуванням “карткових” злочинів;

Другий напрям – це попередження та викриття злочинів, що вчиняються із застосуванням інформаційних технологій, їх розкриття та розслідування.

З метою ефективної протидії злочинам у сфері інформаційно-телекомунікаційних технології та інтелектуальної власності в системі МВС України було запроваджено відповідну спеціалізацію та створено спеціалізовані підрозділи в кожному обласному управлінні.

Протягом п’яти останніх років, з метою виявлення осіб, що намагаються проникати у чужі комп’ютерні мережі, оперативними підрозділами проведено низку оперативно-профілактичних заходів в українському сегменті мережі Інтернет, у телекомунікаційній галузі, а також у сфері електронних платежів; відпрацьовуються комерційні структури, які надають інформаційно-телекомунікаційні послуги в регіонах.

В результаті вжитих організаційних та практичних заходів та завдяки пильній роботі правоохоронних органів була досягнута позитивна динаміка викриття злочинів у сфері високих технологій.

Так, якщо у 2002 році було виявлено лише 16 злочинів у сфері використання комп’ютерів, з яких до суду направлено 9 (56 %), то у 2009 р. виявлено 217 таких злочинів, з них 178 направлені до суду (82 %).

У структурі злочинів, викритих у цій сфері, 26 % складають злочини у сфері інтернет-технологій, 28 % – у сфері функціонування електронних платежів або платіжних карток; 16 % – у сфері телекомунікацій. Решта – пов’язані з використанням комп’ютерних технологій при вчинені традиційних злочинів (підробка документів, грошових знаків, порушення авторських прав тощо).

Третій – напрацювання методик документування і викриття кіберзлочинів, проведення семінарів і тренінгів для працівників практичних підрозділів органів внутрішніх справ.

Для поліпшення методичного забезпечення боротьби зі злочинністю у сфері інформаційних технологій протягом 2002–2010 років узагальнено та опрацьовано позитивний досвід правоохоронних органів інших країн, розроблено та впроваджено у практичну діяльність регіональних підрозділів ДСБЕЗ та в навчальний процес вищих навчальних закладів системи МВС України понад 30 методичних рекомендацій з питань правового забезпечення та документування злочинів у сфері високих технологій. У тому числі науково-практичний коментар до розділу XVI КК України “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж

і мереж електрозв'язку" та навчальний посібник "Правові та організаційні засади протидії злочинам у сфері використання платіжних карток".

Четвертий не менш важливий напрям, пов'язаний з налагодженням ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

В цьому напрямі правоохоронним органам слід налагоджувати взаємодію з банківськими структурами. Однією з форм такої взаємодії є проведення науково-практичних конференцій та семінарів. Слід зауважити, що конференція, організована керівництвом Національного банку України, на якій ми сьогодні присутні, є одним з перших, але вкрай необхідних кроків на шляху створення ефективної системи протидії кіберзлочинам, які вчиняються в сфері банківської діяльності.

В.В. Коваленко, *д-р юрид. наук, проф.,*
член-кореспондент Національної академії правових наук України,
ректор Національної академії внутрішніх справ

ОСВІТНЬО-НАУКОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сьогодні в суспільстві та державі проходять докорінні зміни та перетворення, рішучі й всеосяжні реформи, спрямовані на підвищення конкурентоспроможності економіки, що є єдиним шляхом виходу України на траєкторію сталого розвитку. У значній мірі їх реалізація буде залежати від якісного кадрового забезпечення.

А тому, керівництво держави велику увагу приділяє вирішенню актуальних проблем реформування системи освіти, її доступності, покращенню якості підготовки фахівців.

Ні для кого не буде відкриттям, що випускники вищих навчальних закладів ще не в повній мірі відповідають вимогам роботодавців, а 20 % із них вказують на невідповідність кваліфікації випускників займаній посаді.

Не є виключенням із цього і 13 вищих навчальних закладів системи МВС України, в яких сьогодні лише на денній формі навчається за державним замовленням понад 16 тисяч слухачів і курсантів. Вони здійснюють підготовку фахівців для потреб органів і підрозділів внутрішніх справ за їх основними напрямами діяльності.

Ми розуміємо, що упущеннями в підготовці є певний розрив між рівнем теоретичної підготовки випускників і набутими ними практичними вміннями та навичками. Не секрет, що випускники не завжди

готові після навчання до виконання покладених на них службових обов'язків, особливо в оперативних підрозділах та підрозділах досудового слідства. Є нагальна потреба в підвищенні оснащення навчального процесу технічними засобами, перш за все інноваційними технологіями навчання. І ми постійно працюємо над цими питаннями.

Тож обрана для обговорення проблематика надзвичайно актуальна. Від рівня її опрацювання і нашої взаємодії у реалізації визначених рекомендацій в межах компетенції значною мірою залежатиме фінансово-економічна, а від так і національна безпека держави.

Президент України Віктор Федорович Янукович особливу увагу приділяє консолідації зусиль всіх гілок влади та інституцій, освітян – науковців і практиків в утвердженні в країні верховенства права. Ця теза наголошена і у виступі Глави держави на X позачерговому з'їзді суддів України (16 вересня п.р.).

Характерними для сьогодення є відверті намагання криміналітету взяти під контроль основні напрями господарської діяльності держави. І частково це вдається, про що свідчать викриті численні схеми незаконних оборудок з грошовими коштами, факти легалізації злочинних доходів, розширення мережі фіктивних фірм та "конвертаційних" центрів, злочині у сфері використання високих технологій.

Акцент правопорушень з використанням банківських установ все помітніше переміщується від кредитувань до витоку грошової маси за кордон, відмивання "брудних" коштів шляхом акціонування підприємств, вкладання їх у нерухомість, укладання удаваних угод, повернення незаконно вивезених грошей в якості інвестицій. Особливо турбують шахрайства з банківськими картками, фішінгові атаки тощо.

Політика протидії злочинам у банківській сфері відрізнялася крайньою нестабільністю, відсутністю зваженої науково-обґрунтованої концепції впливу на це явище з загрозливими тенденціями до розповсюдження.

Позначаються прогалини у законодавчому, відомчому та міжвідомчому регулюванні, послаблена взаємодія відповідних органів, відсутність параметрів інформування зацікавлених сторін про порушення, млявість в усуненні причин та умов їх скоєння і недостатній професіоналізм при попередженні і розслідуванні злочинів.

Заступник міністра Леонід Миколайович Зима привернув увагу на необхідність усунення розпорошеності дій і підвищення компетентності правоохоронних структур, налагодження взаємодії правоохоронних органів і банківських структур у протидії кіберзлочинності, з визначенням завдань і ролі у цьому освітян і науковців, аналітиків і практиків.

Робота Міністерства у цьому спрямуванні доведена до відповідних установ і населення засобами масової інформації, на брифінгах

і прес-конференціях, позитивно сприйнята і знаходить зацікавлену підтримку, у тому числі банківськими клієнтами і населенням.

Скажу відверто, що в навчальних закладах МВС України, лише з цього року, з урахуванням вимог Міністра, в навчальному процесу виокремлені питання підготовки кадрів для підрозділів боротьби з кіберзлочинністю та її науково-методичного забезпечення, у тому числі із захисту від таких злочинів банківської системи.

Коротко зазначу і про роль та можливості Національної академії внутрішніх справ у сприянні вирішенню зазначених нагально важливих проблем.

В організаційному плані: на виконання завдань Міністра, вже з другого семестру цього навчального року передбачаємо запровадити нову спеціалізацію підготовки "Протидія кіберзлочинності" шляхом рейтингового відбору на 2–3 курсах найбільш підготовлених і здібних у навчанні курсантів, з навичками поглибленого фахового користування комп'ютерною технікою та вільним володінням іноземною мовою, які виявляють бажання працювати в підрозділах боротьби з кіберзлочинністю, з урахуванням їх працевлаштування (за замовленнями комплектуючих ОВС) у регіонах з широко розвинутими інформаційною інфраструктурою та телекомунікаційними технологіями. Це дозволить вже в найближчі роки без додаткових фінансових витрат отримати кваліфікованих фахівців для роботи у зазначених підрозділах.

Для поглиблення знань, набуття практичних умінь і навичок за запровадженою спеціалізацією до забезпечення навчально-виховного процесу плануємо залучати практичних працівників відповідних підрозділів МВС України:

- стажування випускників плануємо поетапно проводити на базі провідних наукових установ або вищих навчальних закладів міста Києва, які займаються розробкою програмного забезпечення та вдосконаленням функціонування комп'ютерних мереж;
- посилюємо кадровий потенціал профільних кафедр і лабораторій за рахунок докторів наук і професорів, у тому числі за сумісництвом (або контрактом) зі споріднених навчальних закладів, наукових установ і відповідних практичних органів. Розраховуємо на участь у цьому і банківських інституцій;
- розуміючи, що академія в змозі забезпечити належну оперативно-слідчу підготовку фахівців для підрозділів боротьби з кіберзлочинами, ми внесли до МВС пропозицію запровадити з наступного навчального року післядипломну підготовку фахівців з вищою юридичною освітою за спеціалізацією "Протидія кіберзлочинності" із числа осіб, які мають вищу технічну освіту у галузі знань "Інформатика та обчислювальна техніка" – випускники ВНЗ (Національного

технічного університету України "Київський політехнічний інститут", Інституту захисту інформації Державного університету інформаційно-комунікаційних технологій, факультету захисту інформації Національного авіаційного університету тощо) або працівники органів внутрішніх справ з досвідом практичної роботи, з послідуючим проведенням їх юридичної та спеціальної підготовки. Термін навчання може становити 1–2 роки (у залежності від освіти). На наш погляд, підготовка таких фахівців має носити індивідуальний характер з урахуванням практичної їх потреби.

Щодо практичних кроків:

- створена робоча група з розробки освітньо-професійної програми підготовки фахівців за спеціалізацією "Протидія кіберзлочинності" та її науково-методичного забезпечення;
- підготовлений і узгоджується з Департаментом боротьби з кіберзлочинністю та торгівлею людьми МВС України тематичний план підвищення кваліфікації практичних працівників територіальних його підрозділів. Він передбачає отримання слухачами знань і вмінь щодо інформаційної безпеки, особливостей кваліфікації, попередження, виявлення, розкриття та розслідування злочинів у сфері високих технологій (кіберзлочинів), проведення рольових ігор і тренінгів із практичного застосування розроблених нашими фахівцями методик протидії окремим видам злочинів, які вчинюються з використанням комп'ютерних технологій.

Перший такий збір ми готові провести вже з жовтня цього року.

У плані забезпечення навчального процесу за новою спеціалізацією:

- ведеться підготовка навчального плану за новою спеціалізацією з послідуючими погодженнями та розробкою на його базі робочих планів і програм; академія має відповідні ліцензії Міністерства освіти і науки України на здійснення перепідготовки фахівців і підвищення їх кваліфікації. Поряд з навчанням практичних працівників органів внутрішніх справ, відповідно до Постанови Кабінету Міністрів та укладеного з Головним управлінням державної служби України договором, ми здійснюємо підвищення кваліфікації державних службовців, на яких покладені обов'язки з організації роботи щодо запобігання проявам корупції. За 2009–2010 роки кваліфікацію підвищили понад 800 осіб, серед яких представники майже всіх міністерств, інших центральних органів виконавчої влади, органів місцевого самоврядування. При цьому навчання проводиться як у м. Києві, так і в 13 містах, де розміщені регіональні відділення заочного навчання. Ми готові і запрошуємо банківські структури до спільної творчої співпраці (за участю працівників Національного банку України та

фахівців-практиків банківської справи) для проведення підвищення кваліфікації їх працівників за окремими цільовими тематичними планами;

- приділяється увага закріпленню науково-педагогічного складу та підвищення якості забезпечення навчально-виховного процесу – це мають бути дійсно професіонали. Мною дані розпорядження щодо обов'язкового стажування за новою спеціалізацією викладачів у практичних органах, вищих навчальних закладах інших відомств, розраховуємо поділитися досвідом і в установах Нацбанку та його навчальних заклада;
- щодо дидактичного та науково-методичного забезпечення, то підготовлено і вже видано ряд навчальних посібників, підручників, методичних рекомендацій, зокрема, щодо кваліфікації злочинів у сфері використання комп'ютерів, систем і комп'ютерних мереж і мереж електрозв'язку; документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; доказування у справах про злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки; розкриття та розслідування незаконних дій з банківськими платіжними картками; міжнародного співробітництва правоохоронних органів щодо протидії кіберзлочинності; припинення функціонування сайту в мережі Інтернет; встановлення особи, яка розповсюджувала інформацію в мережі Інтернет; основ тактики пошуку інформації кримінального характеру в мережі Інтернет. Їх універсальність використовується як у навчальному процесі, так і безпосередньо у практичній діяльності оперативників. Запрошуємо до авторських колективів і науковців банківської сфери, досвід яких значно посилить прикладний характер подібних знань.

У науковому плані:

- проаналізовано правову регламентацію і практику протидії кіберзлочинності в Україні і за кордоном;
- узагальнено вітчизняний і міжнародний досвід розкриття злочинів відповідного спрямування;
- внесені пропозиції Міністерству внутрішніх справ, Кабінету Міністрів, Верховній Раді щодо поліпшення законодавчого забезпечення протидії злочинам у сфері високих технологій, вдосконалення матеріального і процесуального адміністративно та кримінального права, унормування оперативно-розшукової діяльності;
- готуються дисертаційні дослідження щодо імплементації Україною міжнародно-правових зобов'язань стосовно відповідальності за кіберзлочини та з проблем кримінологічного і криміналістичного аналізу злочинів у сфері використання комп'ютерних технологій.

До речі, у зв'язку із зазначеним, маю поінформувати, що на вимогу Міністра з поточного року кандидатами на здобуття наукового ступеня через ад'юнктуру можуть бути лише особи з практичним досвідом, і ми цього чітко будемо дотримуватися.

Відносно науки додам, що МВС України, його Головне слідче управління, науково-дослідні установи, відомчі вищі навчальні заклади, у тому числі і наша Академія, мають свої фахові видання. В активі періодики "Бюлетень Національного банку України" та "Вісник НБУ", журнали "Банківська справа", "Банківський менеджмент", "Банківська практика за кордоном". Ми ініціюємо робочі зустрічі представників редколегій для узгодження порядку запровадження дискусій, обміну матеріалами та досвідом ефективної взаємодії.

І на завершення: Національна академія внутрішніх справ, зі своєю 90-річною історією, на марші оновлення. У поточному році за всіма формами навчання пройшли державну атестацію понад 5 тисяч правознавців, серед яких і працівників банківських установ всієї України, які навчалися заочно. До того ж, окремі кращі випускники запрошуються на роботу в юридичні підрозділи банківської сфери. І при проведенні занять ми враховуємо такі кадрові перспективи.

На днях на вірність українському народові присягнули понад 800 курсантів вже цьогорічного набору. Ми маємо підготувати нову генерацію працівників української міліції, які на практиці реалізовуватимуть визначений Колегією курс реформи МВС – від репресивних методів до соціально-сервісної функції.

І сьогоднішня конференція також сприятиме виконанню цього важливого державного завдання.

Є.Д. Скулиш, *д-р юрид. наук, доц.,*
ректор Національної академії Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ПРОТИДІЇ КОМП'ЮТЕРНІЙ ЗЛОЧИННОСТІ

Серед найгостріших глобальних проблем, що невідкладно постали сьогодні перед усіма державами, і Україною зокрема, реальну загрозу представляють правопорушення у сфері суспільних інформаційних відносин, що отримали назви "комп'ютерної злочинності", "кіберзлочинності", "комунікаційних злочинів", "злочинів у сфері руху інформації", "злочинів, які вчиняються з використанням комп'ютерних мереж", "злочинів у сфері інформаційно-телекомунікаційних технологій" та інші. Спектр цих злочинів достатньо широкий і постійно зростає,

оскільки дуже стрімко розвиваються та впроваджуються різноманітні інформаційно-телекомунікаційні технології, якими користуються вже сотні мільйонів людей і ця кількість суттєво збільшується з кожним роком.

Так, з метою підвищення темпів розвитку національної культури, освіти, науки, економіки та інших сфер державного та суспільного життя, більшість країн світу розбудовує інформаційне суспільство, значною частиною технологічної складової якого є ресурси і технології мережі Інтернет та сучасні системи телекомунікацій. Відповідно, ми стаємо суттєво залежними від роботи сучасних інформаційно-телекомунікаційних технологій різного призначення, таких як:

- системи стаціонарного та мобільного зв'язку;
- системи електронного документообігу органів державної влади та місцевого самоуправління, організацій та підприємств усіх форм власності;
- системи автоматизованого управління збройними силами та озброєнням;
- системи автоматизованого управління транспортними засобами, об'єктами енергетики та комунікаціями різного призначення;
- державні та приватні електронні бази даних;
- банківські інформаційно-телекомунікаційні системи;
- системи електронної комерції та електронної звітності;
- системи телемедицини та дистанційного навчання;
- персональні комп'ютери, стаціонарні та мобільні телефони громадян;
- та інші.

І як ми бачимо, ця залежність визначається на рівні держави, суспільства та пересічних громадян, яка і обумовлює широкий перелік правопорушень у сфері інформаційно-телекомунікаційних технологій.

Питання протидії комп'ютерній злочинності, безумовно, мають технічний і гуманітарний вимір та відносяться до організаційно-правових, соціальних та технічних заходів інформаційної безпеки. При цьому значна більшість із відомих комп'ютерних злочинів, які стали вже реальністю в Україні, мають економічний характер та представляють собою нові форми неправомірного збагачення шляхом зловживання технологічними можливостями сучасних комп'ютерних мереж та телекомунікацій. Відповідно, зазначені злочини відносяться до сфери компетенції Міністерства внутрішніх справ України та представляють безпосередній інтерес для Національного банку України.

Однак в сучасних умовах масового впровадження комп'ютерних технологій практично у всіх сферах людської діяльності, ми маємо

також справу з такими поняттями як електронне шпигунство, електронне озброєння, електронний тероризм та електронні технології маніпулятивного впливу на свідомість, психологічний та психічний стан громадян. І це є складові загрози сучасного поняття інформаційної безпеки держави, що безпосередньо впливають на стан національної безпеки у всіх її визначальних сферах, включаючи питання благополуччя, життя та здоров'я громадян.

Таким чином, проблема комп'ютерної злочинності має глобальний і національний характер, стосується питань міжнародної та національної безпеки. Відповідно, не визиває сумнівів той факт, що механізми протидії злочинам у сфері інформаційних технологій будуть адекватними сучасним викликам інформаційної безпеки лише за умови реалізації єдиної національної стратегії боротьби з цим ганебним явищем усіма зацікавленими державними структурами, приватним сектором, громадськими організаціями та окремими громадянами з урахуванням існуючої міжнародної практики на рівні ООН, Інтерполу, НАТО та інших організацій.

Система боротьби з комп'ютерною злочинністю – це поняття, що визначає цілісну форму дій усіх учасників цього процесу з метою забезпечення достатнього рівня захисту інформаційних ресурсів та інформаційного простору в сучасних інформаційно-телекомунікаційних системах на національному та міжнародному рівнях. До складових цієї системи можна віднести, насамперед, процес координації зусиль відносно:

- вивчення та класифікації комп'ютерних злочинів, форм та методів їх реалізації;
- стандартизації методів і процедур їх розслідування в різних країнах та співпраці при їх практичній реалізації у відповідних сферах компетенції;
- уніфікації національних законодавств у сфері організаційно-правового, криптографічного та технічного захисту інформації, а також питань моніторингу національних інформаційно-телекомунікаційних систем та регулювання діяльності засобів масової інформації;
- підготовки фахівців у сфері інформаційної безпеки, реалізації просвітницьких заходів щодо попередження комп'ютерних злочинів тощо.

Звісна річ, питання координації зусиль щодо боротьби з комп'ютерною злочинністю – це предмет окремої серйозної дискусії, в рамках доповіді ж пропонується звернути увагу лише на аспект підготовки кадрів у сфері інформаційної безпеки.

Підготовка фахівців з інформаційної безпеки в Україні почалася на початку 90-х років минулого століття на базі технічних вузів із акцентом на технічну діяльність із захисту інформації. На сьогоднішній день Національний технічний університет України "КПІ", Харківський національний університет радіоелектроніки, Державний університет інформаційно-комунікаційних технологій, Національний авіаційний університет та інші технічні вищі навчальні заклади України готують інженерів з питань технічного і криптографічного захисту інформації.

В Європейському університеті, Університеті економіки та права "КРОК" та інших вищих навчальних закладах України готуються фахівці з фінансово-економічної безпеки підприємницьких структур, що мають правову та економічну спеціалізацію.

В свою чергу, Національна академія Служби безпеки України в рамках навчального процесу Навчально-наукового інституту інформаційної безпеки готує фахівців за напрямом підготовки 6.160103 "Організація захисту інформації з обмеженим доступом", а також напрямом підготовки 6.170103 "Управління інформаційною безпекою".

Концептуальна різниця між фахівцями з організації захисту інформації та управління інформаційною безпекою полягає у тому, що у першому випадку пріоритетом є організаційно-правові аспекти захисту різних видів інформації з обмеженим доступом, а у другому – інформаційно-психологічні та технологічні питання інформаційного протиборства.

У загальному випадку, основна особливість Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України (надалі – Інституту) полягає у тому, що ми готуємо фахівців з інформаційної безпеки правової спеціалізації.

З метою формування у студентів розуміння масштабності проблематики інформаційної безпеки, необхідних теоретичних знань та практичних навичок, до навчального процесу залучаються як науковці, так і фахівці практики з питань: права; комп'ютерної техніки та телекомунікацій; організаційно-правового, технічного і криптографічного захисту інформації; засобів і систем захисту об'єктів інформаційної діяльності; психологічних операцій у інформаційному просторі; оперативно-розшукової діяльності; аналітичної роботи; менеджменту захисту інформації; конкурентної розвідки; економічної безпеки підприємств; національної безпеки.

На відміну від інших вищих навчальних закладів, що готують фахівців із інформаційної безпеки, в Інституті основна увага студентів концентрується на нормативно-правових питаннях організації та управління інформаційною безпекою та чіткому розумінні особливостей

усіх професій у цій сфері, їх ролі, місця та завдань у комплексному підході до організації забезпечення належного рівня інформаційної безпеки.

Доцільно також зазначити, що організаційно-правові аспекти протидії комп'ютерній злочинності викладаються в Інституті у спеціальному курсі для магістрів "Організаційно-правові основи захисту банківської таємниці", а технічні – в дисципліні "Комплексні системи захисту інформації".

На завершення, слід також звернути увагу на достатньо актуальну проблему підготовки фахівців із розслідування комп'ютерних злочинів, реалізація якої в класичному технічному або юридичному вищому навчальному закладі здається проблематичною. Оскільки мова йде про підготовку висококваліфікованих інженерів різної спеціалізації, обізнаних з широким колом питань щодо подолання методів технічного і криптографічного захисту інформації, а також одночасно правознавців, фахівців з організації оперативно-розшукової та оперативно-технічної діяльності.

Спираючись на сказане, вважається актуальним питання відкриття нової спеціальності "Організація розкриття й розслідування комп'ютерних злочинів" в рамках існуючих напрямів підготовки навчальних закладів системи Служби безпеки та Міністерства внутрішніх справ України, а також організації плідної міжвідомчої співпраці у процесі підготовки фахівців зазначеної спеціалізації.

Література

1. Інтернет-ресурс (www.crime-research.ru).
2. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека (соціально-правові аспекти): Підручник / За ред. Є.Д. Скулиша. – К., 2010.

О.В. Рибальський, *д-р техн. наук, проф.,*
проф. кафедри інформаційних технологій
Національної академії внутрішніх справ;
В.О. Хорошко, *д-р техн. наук, проф., директор Інституту захисту інформації*
Державного університету інформаційно-комунікаційних технологій;
В.І. Шакун, *д-р юрид. наук, проф., перший проректор з навчальної роботи*
Національної академії внутрішніх справ

КОМПЛЕКТУВАННЯ КАДРАМИ ПІДРОЗДІЛІВ БОРОТЬБИ ЗІ ЗЛОЧИНАМИ У СФЕРІ ВИСОКИХ ТЕХНОЛОГІЙ

Однією з нагальних проблем боротьби з кіберзлочинністю в нашій країні є проблема комплектування висококваліфікованими кадрами спеціалізованих підрозділів, призначених для виявлення та протидії злочинам у сфері високих технологій, які зараз створюються в Україні.

Серед деяких фахівців існує думка, що для розслідування злочинів у сфері високих технологій можна готувати спеціалістів на базі вищої юридичної освіти. Мовляв, для цього слід відбирати курсантів, які мають певні здібності до сучасних інформаційних технологій, та надавати їм методики розслідування таких злочинів. А в разі необхідності, оперативні працівники та слідчі завжди можуть звернутися за допомогою до фахівців у конкретній галузі знань, вибір яких визначатиметься сутністю кожної справи окремо.

Але виникає цілком слушне питання: а хто розроблятиме такі методики? Адже розробка методики вимагає від фахівця власного, поновлювального постійно, досвіду та ґрунтовних наукових знань у тій галузі, в якій розробляється методика.

Слід визнати, що існує ряд методичних рекомендацій, напрацьованих вченими-правознавцями, але вони носять загальний характер та у своїй більшості стосуються питань, не пов'язаних з конкретними методами розслідування "комп'ютерних" злочинів. Це, наприклад, методичні рекомендації щодо вилучення обчислювальної техніки, відкриття кримінальних справ і таке інше.

Крім того, злочинці, які, за правило, є фахівцями в галузі інформаційних технологій, відстежують всі нові досягнення в цій сфері та постійно удосконалюють способи скоєння злочинів.

При цьому майже завжди у злочинців запроваджено "вузьку спеціалізацію": є "фахівці" з підробки банківських карток, зламу та проникненню у банківські інформаційні мережі, зламу баз даних та "добування" персональних даних клієнтів банків, продажу отриманої інформації підробникам банківських карт і т.п.

У своїй діяльності такі злочинці використовують різноманітні способи приховування своїх оборудок та обміну інформацією. Для цього застосовуються сучасні технології захисту інформації при передаванні її по відкритих каналах зв'язку, зокрема, стеганографічні та криптографічні програми захисту при, наприклад, обміну інформацією в мережі Інтернет.

Тому ми вважаємо, що успішно боротися з такими злочинами можуть фахівці, з рівнем фахової підготовки у сфері новітніх технологій не нижчим (а в ідеальному варіанті значно вищим), ніж у злочинців.

З цього витікає, що підрозділи для виявлення злочинів у сфері високих технологій мають комплектуватися спеціалістами в цій галузі техніки. Більш того, ми вважаємо, що необхідно проводити конкурсний відбір за фаховими ознаками на заняття посад у таких підрозділах. При цьому, з урахуванням різновидів злочинних посягань на інформацію та різновидом завдань по боротьбі зі злочинністю в сфері високих

технологій, такі підрозділи мають бути укомплектовані висококваліфікованими фахівцями з наступних технічних напрямів:

- комп'ютерні мережеві та телекомунікаційні системи;
- інформаційні технології;
- криптографічний та стеганографічний захист інформації та криптоаналіз;
- технічний захист інформації та зняття інформації з каналів зв'язку й технічних каналів витоку інформації.

У цій команді мають бути також висококваліфіковані спеціалісти з банківської та фінансової справи. І зрозуміло, що всі ці фахівці крім основної технічної або економічної спеціальності повинні володіти необхідними знаннями у області права та методологією розслідування злочинів.

Ми вважаємо, що готувати кваліфікованих спеціалістів у галузі інформаційних технологій, технічного, криптографічного та стеганографічного захисту інформації у вищих навчальних закладах (ВНЗ) гуманітарного спрямування, якими є ВНЗ МВС України, на теперішньому етапі їх розвитку не лише неможливо, але й непотрібно. Адже для підготовки таких спеціалістів вони повинні пройти повний курс технічного ВНЗ, що вимагатиме від гуманітарних університетів створення бази для організації такого навчання. Без цього фахівці, наприклад, із захисту інформації, будуть "напівфабрикатом". Та й немає сенсу перетворювати гуманітарні ВНЗ у технічні, адже для таких підрозділів потрібні фахівці декількох технічних спеціальностей.

Слід відзначити, що при виявленні таких злочинів фахівці часто стикаються з новими технічними завданнями, оскільки зловмисники постійно удосконалюють способи та засоби своєї "роботи". Вирішення цих завдань у своїй більшості носить складний науково-технічний характер. Такі завдання можуть вирішувати лише висококваліфіковані фахівці.

Кількість фахівців такого плану завжди обмежена, вони не можуть бути продуктом "масового виробництва", що обов'язково відбудеться, якщо готувати спеціалістів для цих підрозділів у ВНЗ МВС.

Та й для їх комплектування потрібна обмежена кількість висококваліфікованих фахівців.

Отже, для забезпечення комплектування кадрами підрозділів по боротьбі зі злочинністю у сфері високих технологій, на нашу думку, необхідно піти шляхом відбору фахівців з числа випускників технічних та економічних ВНЗ з обов'язковою атестацією та подальшим наданням їм необхідних юридичних знань та спеціальних навичок у міліцейських

ВНЗ. Ці знання та навички їм можна надавати у рамках прискореної другої вищої освіти або курсів підвищення кваліфікації.

Але для організації такого спеціалізованого кадрового набору фахівців необхідно на державному рівні вирішити ряд завдань:

1. Створити такі умови служби у цих підрозділах, щоб кращі випускники технічних та економічних ВНЗ намагалися туди потрапити. Для цього, у свою чергу, необхідно:
   - забезпечити високий початковий рівень оплати праці та привілей для таких фахівців, щоб перспективні спеціалісти не шукали роботи у приватних структурах;
   - ввести жорсткі критерії відбору для кандидатів у таки підрозділи та організувати сам відбір так, щоб виключити можливість прийняття на посади людей, що його не пройшли (і цим виключити можливість корупційного прийняття негідних кандидатів на високооплачувані посади);
   - забезпечити такі умови проходження служби, щоб офіцери таких підрозділів були зацікавлені служити як можна довше та не звільнялися через декілька років;
   - заохочувати технічну та наукову діяльність працівників таких підрозділів.
2. Організувати та провести законодавче забезпечення набору кадрів та діяльності таких підрозділів.
3. Організувати широку взаємодію з Міністерством освіти та науки (МОН) і з ведучими технічними та економічними ВНЗ, які готують фахівців із зазначених вище спеціальностей у регіонах, що надасть можливість комплектувати підрозділи місцевими кадрами. Для цього необхідно визначити ВНЗ, які готують студентів за цими спеціальностями з високим рівнем фахової підготовки. При цьому бажано, щоб у цих навчальних закладах велася підготовка офіцерів запасу.

Вирішення цих завдань дозволить швидко провести створення та комплектацію кадрами таких підрозділів.

З часом можна організувати і паралельний шлях підготовки кадрів для таких підрозділів. Ми його вбачаємо у відборі офіцерів міліції, що мають стаж практичної роботи та відповідні здібності на додаткове стаціонарне навчання у ВНЗ технічного та економічного спрямування за потрібними спеціальностями. При цьому у ВНЗ, зайнятих підготовкою таких спеціалістів, необхідно створювати окремі навчальні групи з окремими навчальними планами, оплату навчання проводити державним коштом, а офіцерам на час навчання зберігати вислугу років і все грошове та матеріальне забезпечення.

Зрозуміло, що і при такому шляху підготовки спеціалістів знадобляться і законодавче забезпечення, і взаємодія з МОН.

Нажаль, темпи та напрями розвитку "білокоміркової" злочинності вимагають від нас швидкої організації, створення та забезпечення ефективної діяльності підрозділів протидії цим протиправним зазіханням, які на теперішній час вже складають загрозу політичній, економічній та інформаційній безпеці держави. Тому, на нашу думку, на теперішній час перший шлях видається більш перспективним.

Сподіваємося, що запропоновані нами напрями комплектування кадрів підрозділів для протидії такій злочинності сприятимуть якості їх організації та ефективності функціонування.

О.М. Джужа, *д-р юрид. наук, проф., заслужений юрист України, проректор з наукової роботи Національної академії внутрішніх справ*

ІНТЕРНЕТ-ШАХРАЙСТВО ЯК ОБ'ЄКТ КРИМІНОЛОГІЧНИХ ДОСЛІДЖЕНЬ

На початку 60-х років XX ст. американським юристом Д.Б. Паркер запроваджено термін "комп'ютерна злочинність" для позначення злочинів, у яких комп'ютер є як об'єктом злочину (матеріальна шкода завдається шляхом фізичного пошкодження), так і засобом (коли його використано для вчинення інших злочинів, зокрема шахрайства). "Комп'ютерні злочини" як самостійну групу правопорушень виокремлено учасниками конференції асоціації адвокатів (Даллас, 1979). Пізніше, експерти Організації економічного співробітництва та розвитку (Париж, 1986) дали визначення комп'ютерного злочину, під яким розуміли "будь-яку незаконну, неетичну або заборонену поведінку, яка зачіпає автоматизовану обробку та передачу даних". Цікаво, що у США комп'ютерним злочином вважають будь-яку незаконну дію, для вчинення якої використано знання у галузі комп'ютерних технологій.

Першим міжнародно-правовим документом стосовно цього питання можна вважати Рекомендацію № R89 (9) Комітету Міністрів держав-членів Ради Європи про злочини, пов'язані з комп'ютером, прийняту 13 вересня 1989 р., де вперше сформульовано поняття і визначено перелік комп'ютерних злочинів. У Рекомендаціях № R(95)13 з питань кримінального судочинства підкреслено, що злочини, пов'язані з комп'ютерними технологіями, вчиняються не лише за допомогою комп'ютера, а і комп'ютерних систем чи мереж. На Десятому Конгресі ООН з попередження злочинів і поводження з правопорушниками (Відень, квітень 2000 р.) запроваджено термін "кіберзлочин" як злочин, вчинений в електронному середовищі: засобами комп'ютерних систем і мереж; у

комп'ютерній системі або мережі; проти комп'ютерної системи або мережі.

У даний час чинні кілька міжнародних нормативно-правових актів, що регулюють питання протидії кіберзлочинності. Базовим є Конвенція про кіберзлочинність від 7 вересня 2005 р. За цією Конвенцією до кіберзлочинів пропонується відносити, зокрема, "комп'ютерне шахрайство", тобто навмисне протиправне вчинення дій, що призводять до втрати майна іншої особи шляхом: введення, зміни, знищення чи приховування комп'ютерних даних; втручання у функціонування комп'ютерної системи; набуття, без права на це, економічних переваг для себе чи іншої особи [1]. Ці правопорушення за КК України зазвичай кваліфікують за сукупністю статей: ст. 190 "Шахрайство" та 361 "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку" [2].

Шахрайство в комп'ютерних мережах, зокрема мережі Інтернет, є відносно новим явищем у сучасному світі, вивчення якого у світлі предмета кримінології убачається доцільним з наступних міркувань. По-перше, у кримінологічній науці трапляються лише поодинокі праці, присвячені проблемі шахрайства, що вчиняється за допомогою високих технологій. По-друге, розвиток мережі Інтернет та стрімке удосконалення глобальних комунікацій породжують нові суспільні відносини, зокрема пов'язані з виникненням раніше невідомих видів злочинів. По-третє, загострення уваги на аналізі Інтернет-шахрайства дає змогу систематизувати сучасні підходи до класифікації цього виду злочинної діяльності з метою конкретизації відповідних програм протидії.

Активне упровадження України у світовий інформаційний простір сприяло бурхливому розвиткові комунікаційних технологій, формуванню глобальних комп'ютерних мереж, зростанню індустрії апаратного та програмного забезпечення, комп'ютеризації усіх галузей економіки та повсякденного життя кожної людини. За даними компанії "SputnikMedia.net", на початку 2009 р. у вітчизняній мережі зареєстровано 8,4 млн користувачів Інтернету, а кількість абонентів мобільного зв'язку перевищила 55 млн. [3].

Водночас процеси інформатизації поряд з позитивним впливом на розвиток економіки мають низку негативних наслідків, передусім відкривають широкі можливості для фінансових махінацій. Мережу Інтернет усе більше використовують як засіб незаконного потрапляння до корпоративних та особистих баз даних з метою вчинення різноманітних шахрайських дій. Особливий інтерес злочинців викликає конфіденційна інформація про банківські рахунки та коди доступу до платіжних карток.

За даними МВС України, 2005 р. у сфері електронних платежів було зафіксовано 83 злочини, а 2007 – уже 205. Кількість злочинів, учинених у сфері високих технологій, збільшується прямо пропорційно кількості користувачів комп'ютерних мереж, та, за оцінками Інтерполу, темпи зростання рівня злочинності у глобальній мережі Інтернет є найшвидшими на планеті.

Інтернет-шахрайство, на думку фахівців (Ю.М. Батурін, Д.О. Зиков, С.Г. Спіріна, С.С. Чернявський), є різновидом традиційного шахрайства та становить собою розкрадання чужого майна або набуття права на майно шляхом обману та зловживання довірою, вчинене з використанням мережі Інтернет [4]. Слід підкреслити, що в різних публікаціях для визначення Інтернет-шахрайства застосовують поняття, що нерідко розуміють як тотожні: "комп'ютерне шахрайство", "кібершахрайство", "мережеве шахрайство" та ін. Водночас більшість авторів не наводять критерії розмежування цих понять із суміжними категоріями.

Вважаємо, що для виокремлення інтернет-шахрайства як різновиду фінансового шахрайства слід застосовувати два основні критерії: по-перше, це використання при вчиненні шахрайства можливостей мережі Інтернет; по-друге, це предмет інтернет-шахрайства – кошти фізичних чи юридичних осіб (або права на ці кошти), якими заволодіває шахрай шляхом обману та зловживання довірою (застосовуючи різні прийоми переконання потерпілого свідомо передати шахраям реєстраційні дані своїх платіжних карток або переказати готівку на їх рахунки).

Шахрайську операцію в мережі Інтернет *за віктимологічної ознакою* умовно можна розподілити на три стадії: передача інформації потенційній жертві; безпосереднє заволодіння предметом посягання; усвідомлення жертвою того, що її ошукали через певний проміжок часу (від декількох тижнів до року).

Інтернет-шахрайство пов'язане з іншими злочинними діяннями, зокрема злочинами, передбаченими розділом XVI КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". В окремих випадках ці дії можуть розглядатись як заподіяння майнової шкоди шляхом обману або зловживання довірою (ст. 192 КК України).

Основними ознаками Інтернет-шахрайства є високий ступінь латентності (що більшою мірою пояснюється ставленням жертв); багатоманітність способів вчинення шахрайства (зумовлено широким спектром послуг у мережі Інтернет); глобальний характер (інформаційний простір, на відміну від фізичного, не має чітких кордонів й обмежень); складнощі виявлення та запобігання. Головна складність для кваліфікації дій "віртуальних" аферистів як шахрайства – це встановлення наявності

прямого умислу та корисливої спрямованості діяння. Специфікою Інтернет-шахрайства є відсутність прямого контакту винного з потерпілим.

Інтернет-шахрайство має дві складові: психологічну й технологічну. Психологічна складова впливає на мотивацію потенційної жертви та спонукає її до вчинення дій, яких очікують шахраї. Відповідними засобами впливу можуть бути: прагнення до одержання матеріальної винагороди (швидке збагачення – основа більшості шахрайських пропозицій); намагання безкоштовно одержати платні послуги чи товари (пропозиції безоплатного мобільного зв'язку чи доступу до мережі Інтернет); бажання придбати предмети, які складно чи неможливо придбати в інший спосіб (різні види аукціонного шахрайства та продажу неіснуючих товарів і послуг); жалість й альтруїзм (невідомий розповідає потенційній жертві, що з одним з його близьких сталося лихо, зокрема траплялись випадки, коли шахраї, назвавшись правоохоронцями, вимагали "хабара", щоб затриманий родич "уникнув судимості").

Технологічна складова дає можливість шахраям, по-перше, донести необхідну інформацію до потенційної жертви, по-друге, забезпечити власне анонімність й безпеку, по-третє, одержати від жертви кошти, не вступаючи з нею в безпосередній контакт. Водночас шахраї використовують інформаційно-технічні засоби мережі Інтернет, зокрема: "World Wide Web" або "всесвітнє павутиння", "E-mail", "BBS", електронні платіжні системи ("WebMoney", "PayCash", "Portmone.com", "Яндекс. Деньги"), системи грошових переказів ("Western Union", "Money Gram", "Anelik") тощо.

Серед чинників, що сприяють поширенню Інтернет-шахрайства, можна виокремити такі: відсутність повного або часткового контролю за достовірністю інформації, коректністю поширюваних в електронній мережі даних; відсутність дійової системи обміну інформацією про скарги користувачів мережі Інтернет; відсутність механізму виконання цивільно-правових зобов'язань тощо. Останніми роками серед Інтернет-шахраїв спостерігається тенденція до консолідації шляхом створення злочинних груп і навіть транснаціональних злочинних співтовариств.

Отже, Інтернет-шахрайство – нове явище у вітчизняному кримінальному світі, що має високий рівень латентності та важко виявляється. Складнощі запобігання його виявам зумовлені різними чинниками. Найбільш значущими з них є ті, що визначаються особливостями мережі Інтернет, зокрема відсутністю законодавчого регулювання цієї сфери відносин, неузгодженістю міждержавної взаємодії у боротьбі з комп'ютерними злочинами. У науковому плані є очевидною потреба

проведення цілої низки кримінологічних досліджень проблем запобігання інтернет-шахрайству.

Література

1. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 р. № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.
2. Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : [навч. посіб.] / Карчевський М. В. – К., 2010. – С. 110.
3. Номоконов В. А. Глобализация информационных процессов и преступность / В. А. Номоконов / [Електронрий ресурс] – Режим доступу: http://www.crime-research.org/library/nomokon.htm.
4. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : [монографія] / Чернявський С. С. – К., 2010. – 624 с.

В.В. Коряк, *генерал-майор міліції,*
начальник Департаменту ДСБЕЗ МВС України;
В.І. Василинчук, *кан. юрид. наук, доц.,*
проф. кафедри оперативно-розшукової роботи та спеціальної техніки
Навчально-наукового інституту підготовки кадрів кримінальної міліції
Національної академії внутрішніх справ

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Важливе значення для розвитку та впровадження нових напрямків протидії злочинам у сфері інформаційних технологій, має досвід боротьби зі злочинністю у зарубіжних країнах світу.

У відповідності до положень Європейської конвенції "Про кіберзлочинність", кожна із держав для успішної та ефективної боротьби із злочинністю в сфері інформаційних технологій повинна розробляти і приймати низку процедурних питань щодо виявлення та документування комп'ютерних злочинів.

Як свідчить аналіз досвіду роботи поліції зарубіжних країн, організаційно боротьба зі злочинами у сфері високих технологій забезпечується двома основними способами: покладення додаткових функцій на вже існуючі підрозділи або створення спеціалізованих галузевих служб.

Так, у деяких країнах виконання відповідних функцій покладається на такі галузеві служби як підрозділи боротьби з незаконним обігом наркотиків (Домініканська Республіка), боротьби з організованою злочинністю (Болгарія, Вірменія, Македонія, Монголія, Румунія, Ямайка), боротьби з економічною злочинністю (Алжир, Ангола, Греція, Ізраїль, Індонезія, Ісландія, Колумбія, Латвія, Молдова, Словаччина,

Франція, Хорватія, Японія), боротьби з тероризмом (Угорщина), оперативно-технічного забезпечення (Російська Федерація) тощо.

Виділення підрозділів боротьби зі злочинами у сфері високих технологій у спеціалізовані галузеві служби практикується в таких країнах як Австралія, Бельгія, Білорусь, Великобританія, Данія, Естонія, Індія, Ірландія, Китай, Південна Корея, Литва, Люксембург, Макао, Малайзія, Нідерланди, Німеччина, Норвегія, ПАР, Перу, Польща, Португалія, США, Сінгапур, Словенія, Таїланд, Фінляндія, Чехія, Швейцарія, Швеція тощо [1].

У деяких країнах (Австралія, Білорусь, Німеччина, США) підрозділи боротьби зі злочинами у сфері високих технологій також виконують координаційні функції щодо розслідування кіберзлочинів.

Відповідні спеціалізовані підрозділи поліції Бельгії, Великобританії, США, Чехії окрім основних функцій відповідають за профілактичну та наглядову роботу з виробниками телекомунікаційних послуг.

У Австралії діє Австралійським урядовим комітетом із телекомунікацій (Australian Broadcasting Authority, або ABA) [2], який визначає державну політику Інтернету країни. На офіційному сайті даного державного регулюючого органу радіо, телебачення і Інтернету Австралії розміщена інформація щодо норм і правила національного сегменту Інтернет. Крім того, подана інформація про основні показники роботи провайдерів та інших великих суб'єктів, задіяних в Інтернеті.

При Міністерстві державної безпеки Китаю створено "Центр контролю за шкідливою інформацією", який відповідає за контроль над Інтернетом у Китаї. Даний державний орган презентував нове програмне забезпечення – Internet Police 110 – яке фільтрує контент в Інтернеті [3].

Індійська Служба розслідування кіберзлочинів для виконання своїх функцій також залучає професійних хакерів.

В Англії створено Національний підрозділ по боротьбі з злочинами в сфері високих технологій NHTCU (National Hi-Tech Crime Unit). Даний підрозділ складається із спеціально підготовлених сорока агентів, які перебувають у основному офісі в Лондоні, та сорока шести територіальних слідчих [4].

Основним завданням NHTCU є борьба з організованою кіберзлочинністю, хакерством, яке британським законодавством прирівняне до тероризму, різноманітних фінансових правопорушень з використанням високих технологій, світової мережі Інтернет [3].

У Німеччині підрозділ боротьби зі злочинами у сфері високих технологій та комп'ютерної техніки теж функціонує лише на федеральному рівні, але не обмежується координаційними функціями, а самостійно здійснює відповідні розслідування [1]. Однак в даний момент влада Німеччини веде мову про створення центральне управління по боротьбі

з інтернет-злочинністю. Крім співробітників правопорядку в новій установі також працюватимуть спеціалісти з ІТ-технологій. Другим кроком по боротьбі з інтернет-злочинністю, повинно стати попередження міжнародного консультативного органу. На перших порах Німеччина має намір добитися того, щоб всі країни ЄС в обов'язковому порядку повідомляли владі сусідніх держав про хакерські атаки, появу нових вірусів або випадки інтернет-шахрайства [5].

У Чехії відділ боротьби зі злочинами у сфері високих технологій функціонує наразі лише в центральному апараті Бюро кримінальної поліції та слідчої служби. Проте у найближчому майбутньому планується створення регіональних підрозділів указаної служби.

Окремо хотілося б виділити досвід США, де на законодавчому рівні державні установи зобов'язані повідомляти відповідні федеральні або місцеві підрозділи по боротьбі з кіберзлочинністю про всі випадки несанкціонованого доступу до окремих файлів або баз даних з метою своєчасного реагування на них [1].

США стала однією із перших держав світу, яка вжила заходів щодо кримінальної відповідальності за вчинення злочинів у сфері інформаційних технологій, де дана категорія злочинів з'явилася раніше ніж у інших державах [6, с. 29–31].

Ще в 2000 році ФБР разом з іншими правоохоронними органами створили Центр скарг на шахрайство в Інтернеті. Даний орган був створений для розгляду скарг громадян та юридичних осіб на шахрайські дії в мережі Інтернет, він займається аналітичною роботою щодо шахрайства в мережі, визначає основні тенденції щодо напрямів кіберправопорушень і допомагає правоохоронним органам у виявленні правопорушників [3].

В даний час боротьба з кіберзлочинністю є для чинної адміністрації США одним з пріоритетних завдань. В рамках Міністерства національної безпеки США діє підрозділ, який займається виключно цією проблемою. Нещодавно розроблена спеціальна програма, що отримала назву "Ейнштейн", покликана присікати спроби проникнення хакерів в урядові комп'ютерні мережі. Діє також спеціальний центр з попередження і реагування на кібератаки [7].

Нещодавно Пентагон створив "кібервійсько" – спеціальний підрозділ, який опікується безпекою високотехнологічних систем. У жовтні Міністерство національної безпеки США оголосило про початок програми з набору співробітників до цієї спецслужби. Протягом подальших трьох років на роботу планують найняти тисячу експертів з безпеки [8].

США поряд із такими країнами як Японія та Франція здійснюють розкриття комп'ютерних злочинів за допомогою мобільних провайдерів, хоча це є досить таки не новим методом боротьби проти комп'ютерної

злочинності, відносно наших країн. Так приміром законодавство США зобов'язало усі телефонні компанії, що пропонують платні послуги своїм клієнтам, зберігати записи розмов, які включають імена, адреси і номери телефонів, як мінімум протягом 18 місяців. Представники ФБР вважають, що це допоможе їм розслідувати справи, пов'язані з дитячою порнографією і іншими серйозними злочинами в Мережі. Тобто, ФБР, перевіряє за 18 місяців усе зведення абонента мобільного зв'язку, який показався ним підозрілою. Таким чином, вони обчислюють номери телефонів на які абонент здійснював дзвінки, тим самим визначають коло підозрюваних осіб в скоювання подібних злочинів. Вивчаю кількість користувачів і постійних клієнтів, тим самим виходять на замовників цієї продукції.

Більше того ФБР має намір зобов'язати інтернет-провайдерів США зберігати як мінімум протягом двох років дані про усі сайти, що відвідуються користувачами [9].

У структурі МВС Російської Федерації у 1998 році створено Управління по боротьбі зі злочинами у сфері високих технологій, на яке було покладено принципово нові завдання та функції, визначені російським кримінальним законодавством і міжнародними зобов'язаннями Російської Федерації [3]. Два роки було затрачено на формування аналогічних підрозділів на місцях. Територіальний підрозділи були сформовані та функціонують з 2000 року на території 81 суб'єкту РФ [10].

Значну увагу боротьбі із злочинами в сфері інформаційних технологій уділяє Європейський союз. Європейське агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA). – підрозділ по боротьбі з кіберзлочинністю, що координує та об'єднує зусилля поліції країн-учасників ЄС. ENISA виникає після прийняття Постанови (ЄС) № 460/2004 Європейського Парламенту та Ради від 10 березня 2004.

Створюючи таку організацію члени ЄС зазначали, що Агентство створюється не для того, щоб бути єдиним підрозділом по боротьбі з кіберзлочинністю у всій Європі, а як загальний дослідницько-аналітичний і освітній центр, де регіональні підрозділи визначених національних правоохоронних органів будуть централізовано зберігати матеріали і дані для більш ефективного їхнього використання. Одне з завдань створення ENISA – підвищення обізнаності держави, бізнес-сектора і суспільства в цілому щодо загроз безпеки, що поширюють віруси і ворожі коди. До завдань Агентства входить розв'язання всіх проблем, пов'язаних із інформаційною безпекою як для урядових організацій, так і для потужних ділових структур [11].

Також необхідно зауважити, що в більшості країн на базі підрозділів боротьби зі злочинами у сфері високих технологій або НЦБ Інтерполу створено контактні пункти з питань протидії комп'ютерній злочинності, які покликані забезпечувати оперативну взаємодію правоохоронних органів різних країн у розслідуванні відповідних злочинів [1].

Література

1. Аналітичний огляд організації роботи поліції зарубіжних країн щодо протидії злочинам у сфері високих технологій // Матеріали з сайту Укрбюро Інтерполу [Електронний ресурс]. – Режим доступу: http://26308.ncbinter.web11.ukraine.com.ua/?p=275.
2. Спецслужбы задержали интернет-мошенников из Украины // Матеріали з сайту Корреспондент.net [Електронний ресурс]. – Режим доступу: http://www.korrespondent.net/main/93952.
3. Всеукраїнський прес-центр Німеччина створює центральне управління по боротьбі з інтернет-злочинністю // Матеріали з сайту Всеукраїнський прес-центр [Електронний ресурс]. – Режим доступу: http://presscenter.ukrinform.ua/news-48879.html.
4. Державне регулювання суспільних відносин в мережі Інтернет // Матеріали з сайту referaty.pp.ua [Електронний ресурс]. – Режим доступу: http://www.referaty.pp.ua/abstracts/ua/pravo/pravo_23914.php.
5. Історія виникрення та напрямки діяльності // Офіційний сайт МВС Російської Федерації [Електронний ресурс]. – Режим доступу: http://www.mvd.ru/struct/upravleniek/10000288/.
6. Китай почав готуватися до кібервійни зі США технологій // Матеріали з сайту ТСН.ua [Електронний ресурс]. – Режим доступу: http://weather.tsn.ua/svit/kitai-pochav-gotuvatisya-do-kiberviini-zi-ssha.html.
7. Офіційний сайт Australian Broadcasting Authority / Режим доступу: www.aba.gov.au.
8. Офіційний сайт ENISA – Securing Europe's Information Society [Електронний ресурс]. – Режим доступу: http://www.enisa.europa.eu.
9. Раскрытие преступлений с помощью мобильных провайдеров // Матеріали з сайту CyberCrime [Електронний ресурс]. – Режим доступу: http://cybercrime.zp.ua/viewtopic.php?f=10&t=4502#p10672.
10. У США розпочався набір персоналу кібервійськ // Матеріали з сайту ТСН.ua [Електронний ресурс]. – Режим доступу: http://tsn.ua/svit/u-ssha-rozpochavsya-nabir-personalu-kiberviisk.html.
11. О некоторых мерах борьбы с киберпреступлениями в США // Борьба с преступлениями за рубежом. – 2001. – № 7. – с. 29–31.

Ю.Ю. Орлов, *д-р юрид. наук, ст. науковий співробітник,*
проректор з науково-методичної роботи
Національної академії внутрішніх справ

ПРОБЛЕМИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ВЧИНЕННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Під терміном "кіберзлочинність" розуміють сукупність злочинів, які вчиняють із застосуванням інформаційних технологій. При цьому злочинці використовують, здебільшого, можливості глобальної комп'ютерної мережі Інтернет, що надає кіберзлочинам транснаціонального характеру. Отже, боротьба з комп'ютерною злочинністю вимагає скоординованої діяльності усіх країн на основі укладання відповідних міжнародних угод.

Міжнародна конвенція "Про кіберзлочинність", підписана 23 листопада 2001 року у місті Будапешті, стала важливим правовим документом, на базі якого держави, що приєдналися до неї, розбудовують власні системи протидії злочинам, що вчиняють шляхом застосування інформаційних технологій.

Конвенція передбачає чотири групи злочинів, пов'язаних із використанням комп'ютерних технологій як інструменту їх вчинення. До першої групи конвенція відносить злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв та комп'ютерних програм). До другої групи – злочини, пов'язані з використанням комп'ютерних засобів (підробка, шахрайство). До третьої групи віднесені злочини, пов'язані зі змістом даних (дитяча порнографія). До четвертої – злочини, пов'язані з порушенням авторського права та суміжних прав.

При цьому держави, які приєдналися до конвенції, взяли на себе зобов'язання переглянути своє законодавство з метою приведення його у відповідність до рекомендацій, викладених у цьому міжнародному документі.

Аналіз чинного законодавства України дозволяє дійти висновку, що за більшість злочинів, зазначених у конвенції, в нашій країні існує кримінальна відповідальність.

Так, розділ XVI КК України містить низку статей, що передбачають кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку:

- стаття 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку);
- ст. 361^1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут);
- ст. 361^2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації);
- ст. 362 (несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї);
- ст. 363 (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється);
- ст. 363^1 (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку).

На виконання вимог конвенції до розділу XVI КК України Законом України від 5 червня 2003 року № 908-IV були внесені відповідні зміни.

Разом з тим, перелік кіберзлочинів не вичерпується діяннями, зазначеними у розділі XVI КК України. Виявляється, що певні злочини, які існували задовго до виникнення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. При цьому використання комп'ютерів зазвичай спрощує вчинення злочину або уможливлює його вчинення в нових формах. Отже, ці злочини можна розглядати як такі, що підпадають під дію конвенції. Зокрема, йдеться про наступні злочинні діяння:

- різні види підробки: грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору, контрольних марок, номерів вузлів та агрегатів транспортних засобів, документів на отримання наркотиків, інших документів тощо (ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України);
- шахрайство з різними об'єктами (ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України);

- ввезення, виготовлення, збування і розповсюдження порнографічних предметів (ст. 301 КК України);
- порушення авторського права і суміжних прав (ст. 176 КК України).

Природно поставити питання, а чи враховані всі вимоги конвенції у чинному кримінальному законодавстві України. Для відповіді на нього слід встановити відповідність між статями конвенції та статями Кримінального кодексу України. Така відповідність надана в таблиці, аналіз змісту якої дозволяє в цілому стверджувально відповісти на поставлене питання. Водночас слід зробити два зауваження.

Перше зауваження стосується того факту, що в Україні передбачена кримінальна відповідальність й за інші діяння, що можуть бути вчинені шляхом застосування інформаційних технологій, проте відсутні в тексті міжнародної конвенції.

Можна виділити дві групи цих діянь. До першої слід віднести злочини, які полягають у незаконному придбанні та (або) збуті через мережу Інтернет предметів, заборонених для вільного обігу:

- незаконне придбання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307 КК України);
- незаконне придбання чи збут вогнепальної зброї, бойових припасів, вибухових речовин; збут холодної зброї (ст. 263 КК України);
- придбання радіоактивних матеріалів (ст. 265 КК України).

Таблиця 1

№статті конвенції	**Зміст статті конвенції**	**Відповідність статтям КК України**
Злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем		
2	Протизаконний доступ	Статті 361, 363
3	Протизаконне перехоплення	Статті 362, 363
4	Вплив на дані	Статті 361, 362, 363[1]
5	Вплив на функціонування системи	Статті 361, 361[1], 362, 363, 363[1]
6	Протизаконне використання пристроїв та комп'ютерних програм	Статті 361[1], 362, 363
Злочини, пов'язані з використанням комп'ютерних засобів		
7	Підробка з використанням комп'ютерних технологій	Статті 199, 200, 215, 216, 224, 290, 318, 358, 366
8	Шахрайство з використанням комп'ютерних технологій	Статті 190, 192, 222, 262, 308, 312, 313, 357, 410
Злочини, пов'язані зі змістом даних		

9	Злочини, пов'язані з дитячою порнографією	Стаття 301
Злочини, пов'язані з порушенням авторського права та суміжних прав		
10	Злочини, пов'язані з порушенням авторського права та суміжних прав	Стаття 176

До другої групи діянь належать злочини, пов'язані зі змістом даних (контентом). Конвенція розуміє під незаконним контентом виключно дитячу порнографію.[6] Разом з тим, законодавство України дозволяє вважати злочином розміщення в Інтернеті також інформації іншого характеру, а саме:

- відомостей, що становлять державну або іншу таємницю, яка охороняється законом: незаконне розголошення лікарської таємниці (ст. 145 КК України), порушення таємниці голосування (ст. 159), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення комерційної таємниці (ст. 232), розголошення державної таємниці (ст. 328), несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2), розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381), розголошення даних досудового слідства та дізнання (ст. 387), розголошення відомостей військового характеру, що становлять державну таємницю (ст. 422);
- завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК України);
- закликів до вчинення дій, які загрожують громадському порядку (ст. 95 КК України);
- пропаганди расової, національної, релігійної нетерпимості (ст. 161), культу насильства і жорстокості (ст. 300) або війни (ст. 436 КК України);
- спаму, тобто масового розповсюдження повідомлень з метою перешкоджання роботі комп'ютерів, автоматизованих систем чи комп'ютерних мереж (ст. 363^1 КК України).

До третьої групи діянь слід віднести легалізацію (відмивання) грошових коштів, здобутих злочинним шляхом (ст. 209 КК України). Для цього злочинці застосовують послуги електронних банків, надають рахунки на завищені або занижені суми, беруть участь у кібераукціонах тощо.

[6] Окремим протоколом до конвенції охоплюється також расизм та ксенофобія.

Друге зауваження полягає в тому, що деякі позиції конвенції досі не знайшли відображення у вітчизняному кримінальному законодавстві. Так, КК Україні не передбачає кримінальної відповідальності за:

- придбання шкідливих комп'ютерних програм та пристроїв, створених чи адаптованих для вчинення комп'ютерних злочинів (п/п. I п. "a" ч. 1 ст. 6 конвенції);
- виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання у користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром використати їх з метою вчинення комп'ютерних злочинів (п/п. II п. "a" ч. 1 ст. 6 конвенції);
- володіння вище зазначеними шкідливими комп'ютерними програмами, пристроями, комп'ютерними паролями, кодами доступу чи іншими аналогічними даними (п. "b" ч. 1 ст. 6 конвенції);
- придбання дитячої порнографії через комп'ютерну систему (п. "d" ч. 1 ст. 9 конвенції);
- володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних (п. "e" ч. 1 ст. 9 конвенції).

Запровадження кримінальної відповідальності за більшість з вказаних діянь кожна держава – учасник конвенції має право визначати самостійно. Тому необхідність криміналізації цих діянь визначається ступенем їх суспільної небезпеки в умовах України та кримінологічними характеристиками: рівнем, динамікою тощо.

Водночас, зміст ч. 3 ст. 6 конвенції контекстуально зобов'язує всі держави, що приєдналися до неї, ввести кримінальну відповідальність за продаж, оптовий продаж чи інші форми надання у користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути вчинений комп'ютерний злочин. Відповідальність за ці діяння в Україні не встановлена. Разом з тим, поширення практики викрадення та продажу злочинцям комп'ютерних паролів і кодів доступу особами, що мають доступ до них у зв'язку зі своїми службовими обов'язками, неодмінно призведе до зростання кількості комп'ютерних злочинів, значно полегшуючи їх вчинення.

Серед таких злочинів – вчинення крадіжок із використанням підроблених платіжних карток, шахрайств, пов'язаних із функціонуванням Інтернет-магазинів, наданням послуг мережею Інтернет, незаконне отримання персональних даних, несанкціоноване проникнення у корпоративні комп'ютерні мережі з метою блокування їх роботи, отримання конфіденційної інформації, отримання доступу до грошових коштів банку тощо.

Вирішення зазначеної проблеми має стати актуальним завданням для подальшої законотворчої роботи у сфері боротьби з кіберзлочинністю.

О.П. Лебедєв, *канд. юрид. наук,*
начальник ВСМ УМВС України в місті Севастополі

ПІДГОТОВКА ФАХІВЦІВ ПРАВОХОРОННИХ ОРГАНІВ ПО БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Актуальність проблеми підготовки фахівців правоохоронних органів по боротьбі з кіберзлочинністю полягає в належній забезпеченості відповідними фахівцями правоохоронних органів та їх підготовки в сфері протидії несанкціонованому втручанню за допомогою шкідливих програмних засобів в електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку, а також в комплектації таких органів фахівцями в сфері інформаційних технологій та захисту інформації.

Вирішення проблеми підготовки фахівців і комплектування правоохоронних органів певною мірою задовольнить потреби як науки (теоретичні розробки захисту інформації), так і практики (захист інформації як предмета злочинного посягання) та буде сприяти підвищенню ефективності захисту інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах та мережах електрозв'язку, ефективного викриття, документування, розкриття та розслідування злочинів у цій сфері. Проблему підготовки фахівців правоохоронних органів по боротьбі з кіберзлочинністю вивчали: Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, А.В. Іщенко, В.С. Цимбалюк, В.Г. Хахановський та інші вчені, які займалися розробкою питання протидії кіберзлочинності.

У відомчих вищих навчальних закладах системи МВС на даний час розроблені і активно вивчаються слухачами та курсантами навчальні програми з розслідування комп'ютерних злочинів, а також проводяться навчання співробітників МВС з питань розслідування злочинів у сфері інформаційних технологій та організації оперативно-розшукової роботи на основі інформаційних технологій.

Відповідно до Закону України "Про основи національної безпеки України" [1] наша держава реалізує Комплексну програму по усуненню загроз національній безпеці в різних сферах, в тому числі й в інформаційній. Приоритетним напрямом цієї діяльності є комп'ютерна злочинність та комп'ютерний тероризм. Без сучасного захисту інформації в елетронно-обчислювальних машинах (комп'ютерах), автоматизованих

системах, комп'ютерних мережах та мережах електрозв'язку не може бути забезпечена національна безпека нашої держави. У зв'язку з цим постає проблема не тільки браку самих знань, а й кадрового забезпечення підрозділів професіоналами. Відомчі навчальні заклади системи МВС України проводять підготовку фахівців правоохоронних органів у сфері боротьби з кіберзлочинністю. Але така підготовка не повною мірою відповідає потребам сьогодення та оперативної обстановки в регіонах.

Проблеми вищої освіти в Україні з підготовки фахівців у сфері інформаційних технологій неодноразово досліджувались у фахових виданнях. Це і низька заробітна плата професорсько-викладацького складу, практична відсутність матеріального забезпечення навчального процесу, дефіцит сучасної навчальної літератури, відірваність від світових джерел наукової інформації у сфері боротьби з кіберзлочинністю. Вихід з такої ситуації вбачається в розробці загальнодержавної програми підготовки фахівців. На думку інших дослідників, основним недоліком процесу підготовки фахівців називається відсутність єдиної стратегії боротьби з цими злочинами та безсистемність в організації процесу підготовки та перепідготовки кадрів у цій сфері [2].

Підготовку фахівців у сфері інформаційних технологій необхідно продовжувати у напряму реформування діяльності відомчих закладів освіти МВС України з підготовки та перепідготовки фахівців: оперативних співробітників, слідчих, експертів. Постійно проводити перегляд навчальних планів, введення таких предметів, як правова інформатики та інформаційно право, а також нових спеціалізацій з інформаційно-аналітичного забезпечення діяльності ОВС, захисту відомчої інформації і боротьби з кіберзлочинністю. Освітньо-професійні плани навчання повинні входити до затверджених галузевих стандартів вищої освіти, тобто визначення сучасних напрямів підготовки фахівців по боротьбі з кіберзлочинністю. Такий фахівець повинен мати належну підготовку не тільки з юридичних дисциплін, а й природничо-наукових: фізики, математики, інформатики, достатніх для розв'язання завдань у сфері боротьби з комп'ютерною злочинністю, знання обчислювальних середовищ, прикладних програм, технічних аспектів організації захисту інформації.

У сучасних умовах співробітники правоохоронних органів не можуть достатньою мірою тримати в полі зору всі технічні нововведення, що стрімко розвиваються в інформатиці. Готуючи таких співробітників, одним з основних завдань, на нашу думку, є відслідковування новітніх інформаційних технологій, розробка нових методик захисту інформації з застосуванням таких методик на практиці. Підготовка фахівців, які протистоять кіберзлочинності повинна проводитись з урахуванням

міжнародного досвіду зарубіжних правоохоронних органів, досягнень у протидії такого виду злочинів. Накази Генеральної прокуратури України чітко зазначають міжнародне співробітництво в роботі органів прокуратури, мета якого – удосконалення механізмів та процедур надання правової допомоги й обміну досвідом, встановлення й розвиття контактів з компетентними установами іноземних держав і міжнародними організаціями [3, с. 99]. Практичний бік цього співробітництва реалізується у вигляді зустрічей, переговорів, конференцій, семінарів, реалізації проектів і програм співпраці.

Вивчивши потреби практики, вищі навчальні заклади повинні мати сучасні навчальні програми для слідчих, оперативних та експертних підрозділів. Готувати фахівців відповідно до державного замовлення цим органам. Необхідно уважно вивчати вимоги підрозділів, що ведуть боротьбу з несанкціонованим втручанням в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку. Необхідність підготовки фахівців у сучасних умовах полягає в тому, що сама сфера інформаційних технологій розвивається стрімковими темпами, розробляються та впроваджуються нові системи для передачі даних, технічні стандарти та інше.

Крім цього при підготовці фахівців необхідно звертати увагу і на зміни законодавства в даній сфері. Відповідно до ст. 35 Європейської конвенції про кіберзлочинністю від 23 листопада 2001 р. ратифікованої Верховною Радою України 7 вересня 2005 р. необхідно створити спеціальний орган. Який зміг би координувати роботу щодо протидії кіберзлочинності для цілодобових контактів з метою надання негайної допомоги в розслідуванні чи переслідуванні кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів в електронній формі, що стосується кримінального правопорушення. Актуальною проблемою в підготовці спеціалістів, що займаються боротьбою із злочинністю у сфері інформаційних технологій, є збереження та поповнення викладацьких кадрів, підтримання їх на належному професійному рівні. Не останнє місце в матеріально-технічному забезпеченні навчального процесу займає поповнення таких кафедр талановитою молоддю, створення умов для їх ефективного навчання в сфері інформаційних технологій, належне забезпечення кафедр та навчальних аудиторій комп'ютерною технікою, підвищення заробітної плати викладацькому складу відповідно до професійних здобутків, якостей з підготовки та проведення навчального процесу.

Таким чином, реалії сьогодення вимагають від держави вжити своєчасні й адекватні заходи з протидії злочинності в сфері інформаційних технологій; суттєвим кроком у цьому напрямі може стати розро-

бка і прийняття загальнодержавної програми підготовки таких фахівців. Необхідно на належному рівні забезпечити навчальний процес для таких фахівців: це і матеріальне забезпечення майбутніх фахівців сучасною навчальною літературою не тільки вітчизняних, а й зарубіжних авторів, а також забезпечення інформацією щодо передових інформаційних технологій та розробок у сфері захисту інформації. Підготовка фахівців правоохоронних органів по боротьбі з кіберзлочинністю повинна здійснюватися як досвідченими науковцями, так і практичними співробітниками. Також доцільно здійснити організацію поповнення кафедр молодими спеціалістами, що мають як теоретичні, так і практичні напрацювання в цій сфері.

Література

1. Закон України "Про основи національної безпеки України" від 19 червня 2003 року № 964-IV, Відомості Верховної Ради України, 2003. [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua.
2. Бєляков К.І. Підготовка фахівців у сфері інформаційної безпеки: стан в Україні [К.І. Бєляков, В.Д.Гавловський] // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2005. – № 12 // [Електронний ресурс]. Режим доступу: mndc.naiau.kiev.ua/Gurnal/12.htm$.
3. Гуцалюк М.В. Міжнародне співробітництво щодо протидії злочинам у сфері інформаційних технологій. // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2003. – № 8. – С. 97–104.

Г.С. Севрюкова, *ст. оперуповноважений ВСМ УМВС України в м. Севастополі, ад'юнкт Національної академії внутрішніхсправ*

СУЧАСНИЙ СТАН БОРОТЬБИ ЗІ ЗЛОЧИНАМИ У СФЕРІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Людська цивілізація на межи тисячоліть вступила в еру інформації. З кожним днем активніше розвиваються сучасні інформаційні технології і в Україні [1, 6]. Основні напрями науково-технологічного розвитку України спрямовані на вирішення проблем та визначення перспектив розвитку суспільства. Верховна Рада України визначила одним із стратегічних пріоритетних напрямів інноваційної діяльності в Україні на 2003–2013 роки нанотехнології, мікроелектроніку, інформаційні технології, телекомунікації [2, 9].

Комп'ютерні технології використовуються практично в усіх сферах та галузях зв'язку, енергетики, транспорту, державними органами та багатьма іншими установами [3, 77]. Разом з тим, розвиток інформаційного суспільства супроводжується негативними процесами протиправного використання інформаційних і телекомунікаційних технологій. Кількість злочинів, вчинених у кіберпросторі, росте пропорційно кількості користувачів комп'ютерних мереж, і, по оцінках Інтерполу, темпи

зростання злочинності в глобальній мережі Інтернет є найшвидшими на планеті [4, 36].

Для України, яка має значний потенціал передових наукових знань, новітніх технологій, проблема їх захисту від несанкціонованого доступу є надзвичайно актуальною. Правоохоронними органами України спільно з іншими державними та недержавними структурами постійно виявляються і документуються злочині, які вчиняються за допомогою комп'ютерних технологій, у тому числі у сфері кредитно-банківської системи. Ефективний захист прав інтелектуальної власності та протидія комп'ютерній злочинності є одним з пріоритетних напрямів діяльності правоохоронних органів у сфері забезпечення економічних інтересів держави.

В той же час науковці та законодавці використовують й інші назви злочинів, пов'язаних з використанням інформаційних технологій, які теж мають прикметник "комп'ютерний": інформаційні комп'ютерні злочини (В.В. Крилов); злочини у сфері комп'ютерної інформації (Кримінальний кодекс РФ); злочини у сфері високих технологій і комп'ютерної інформації (А.В. Варданян); злочини, що вчиняються за допомогою комп'ютерних технологій (Б.В. Романюк, В.Д. Гавловський); злочини у сфері використання комп'ютерних технологій (В.О. Голубєв, В.С. Цимбалюк); злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Кримінальний кодекс України) [5, 54].

На виконання Указу Президента України від 27.04.2001 № 285/2001 "Про заходи щодо охорони інтелектуальної власності" у 2001 році в структурі Державної служби боротьби з економічною злочинністю МВС України були створені підрозділи по боротьбі з порушеннями у сфері інтелектуальності та високих технологій, як в центральному апараті, так і на регіональному рівні. Основними завданнями цих підрозділів є попередження і викриття правопорушень у сфері інтелектуальної власності, створення і вдосконалення необхідної для протидії цим явищам законодавчої бази. Як підкреслює досвідчений фахівець Л.П. Скалозуб, "аналіз криміногенної ситуації у цій сфері свідчить, що найбільш поширеними видами злочинів є: шахрайство з використанням комп'ютерної техніки, у тому числі в мережі Інтернет (ч. 3 ст. 190 КК України), несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж (ст. 361 КК України) та підроблення і шахрайське використання платіжних карток, ініціювання неналежних електронних грошових переказів (ст. 200 КК України)" [6, 11].

Динамічний розвиток ринку електронних платежів в України протягом останніх років створив сприятливі передумови для розвитку такого злочинного бізнесу, як викрадення конфіденційної інформації про емітовані банківськими установами платіжні картки та використання

такої інформації для виготовлення підроблених карток чи проведення розрахунків з використанням чужих банківських реквізитів в торгівельній мережі (або ж в мережі Інтернет-розрахунків). Вивчення стану криміногенної ситуації у сфері функціонування електронних платіжних систем свідчить про значне поширення протиправної діяльності з використанням платіжних карток, у т.ч. виявлення в банкоматній мережі пристроїв для незаконного зчитування інформації про платіжні картки законних держателів, яка використовується для їх підроблення та отримання за ними грошових коштів. На сьогодні в Україні діє 196 банківських установ, із яких 128 є членами внутрішньодержавних і міжнародних карткових платіжних систем та здійснюють емісію і еквайрінг платіжних карток [7, 97].

Відсутність спеціального регулювання обігу пластикових платіжних засобів та регламентації обов'язків їх утримувачів призводить до того, що в одних випадках учасники ринку пластикових карток не повідомляють правоохоронні органи про відомі їм факти злочинних посягань, покриваючи збитки за рахунок власних ресурсів. В такий спосіб вони намагаються підтримати рівень ділової репутації, а також уникнути втручання контролюючи і правоохоронних органів в свою комерційну діяльність. В інших випадках співробітники правоохоронних органів помилково оцінюють злочинні посягання, як цивільно-правові делікти. Як зауважує Л.Л. Тимченко, "важко складати прогнози відносно кількості шахрайств з пластиковими платіжними картками. З упевненістю можна сказати тільки те. що суми збитків від них продовжують збільшуватися. Правоохоронні органи мають можливість формувати статистик тільки на основі виявлених злочинів, вилучених підроблених карток та порушених кримінальних справ. Велика частина підроблених карток так ніколи і не вилучається, що зумовлює високу ступень латентності цього виду злочинів" [7, 98].

Пропонуємо основні напрями, за якими необхідно будувати взаємодію між правоохоронними органами і службами безпеки платіжних систем:

- своєчасне виявлення фактів злочин посягань, пов'язаних з використанням пластикових платіжних засобів;
- швидке і ефективне реагування на виявлені факти злочинних посягань;
- швидке і безпроблемне отримання необхідної інформації в міжнародних платіжних системах;
- взаємні консультації, відповідно до повноважень;
- обмін інформацією, зокрема, ведення спеціальних обліків;
- допомога у зборі доказів по фактам правопорушень;

- аналітична робота, створення методологічної бази, навчання, законодавчі ініціативи;
- здійснення загальних профілактичних заходів. Найкраще взаємодія і співпраця правоохоронних органів і служб безпеки платіжних систем побудована в тих країна, де їх взаємні зобов'язання максимально формалізовані на законодавчому рівні. Така практика притаманна більшості розвинутих країн, в яких "картковий" бізнес контролює величезні фінансові потоки і є складовою повсякденного життя. Інший варіант організації взаємодії, наприклад в Росії, передбачає визначення взаємних зобов'язань на договірній основі [7, 98–99].

Підсумовуючи сказане, доходимо до висновку, що всі економічні злочини, в тому числі і з використанням пластикових платіжних засобів, відносяться до категорії латентних, однак в теперішній ситуації співробітники правоохоронних органів за наявності відповідної підготовки, а також організаційних зусиль можуть успішно протидіяти злочинним посяганням, використовуючи норми чинного Кримінального кодексу України.

Література

1. Біленчук П.Д. Комп'ютерна злочинність. [П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін.] Навчальний посібник. К: "Атіка", 2002. – 240 с.
2. Бутузов В.М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки [В.М. Бутузов, В.Д. Гавловський, Л.П. Скалозуб, К.В. Тітуніна, В.П. Шеломенцев]. Науково-практичний посібник за заг. ред. Л.П. Скалозуба, І.В. Бондаренко. – К, 2010. – 245 с.
3. Савченко О.В. Документування несанкціонованого втручання в роботу автоматизованих систем та мереж електрозв'язку, що призвело до блокування інформації (DDOS-атаки) / Відп.ред. Л.П. Скалозуб, В.І. Василинчук, С.А.Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009 р.: тези допов. – К., 2009. – 114 с. (С. 77–82).
4. Гавловський В.Д., Тітуніна К.В. Актуальні питання міжнародного співробітництва у боротьбі з комп'ютерною злочинністю. / Відп. ред. Л.П. Скалозуб, В.І. Василинчук, С.А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009р.: тези допов. – К., 2009. – 114 с. (С. 36–42).
5. Шеломенцев В.П. Щодо використання терміну "Комп'ютерні злочини" / Відп. ред. Л.П. Скалозуб, В.І. Василинчук, С.А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009 р.: тези допов. – К., 2009. – 114 с. (С. 53–58).
6. Скалозуб Л.П. Стан захисту прав інтелектуальної власності та протидія комп'ютерній злочинності, проблемні питання і шляхи їх вирішення. / Відп. ред. Л.П. Скалозуб, В.І. Василинчук, С.А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009 р.: тези допов. – К., 2009. – 114 с. (С. 5–12).

7. Тимченко Л.Л. Характеристика злочинів, що вчиняються з використанням підроблених платіжних карток / Відп. ред. Л.П. Скалозуб, В.І. Василинчук, С.А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009 р.: тези допов. – К., 2009. – 114 с. (С. 97–100).

Е.В. Рижков, *канд. юрид. наук, доц.,*
начальник кафедри оперативно-розшукової діяльності
Донецького юридичного інституту ЛДУВС імені Е.О. Дідоренка

ДОСВІД ПІДГОТОВКИ КАДРІВ ДЛЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ПО БОРОТЬБІ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ

На базі Донецького юридичного інституту ЛДУВС ім. Е.О. Дідоренка в рамках спеціалізації "оперативно-розшукова діяльність у сфері інформаційних технологій" з 2001 року здійснюється підготовка фахівців з протидії злочинам, пов'язаним із використанням комп'ютерних мереж. Щорічно з усіх областей України та Автономної республіки Крим здійснюється набір абітурієнтів в кількості 25 осіб.

Підготовка фахівців здійснюється на кафедрі оперативно-розшукової діяльності факультету кримінальної міліції. Науково-викладацьким складом інституту в рамках зазначеної спеціалізації було розроблено методичне забезпечення з наступних навчальних дисциплін: Інформаційне право, Інформаційна техніка, технології та їх програмне забезпечення, Інформаційна безпека, Інформаційні технології в банківській діяльності, Оперативно-розшукова діяльність у сфері інформаційних технологій, Аналітична розвідка, Технічна розвідка.

До штату кафедри входить 10 осіб, з яких 9 – науково-викладацького складу. Штат повністю укомплектований фахівцями, які працюють на постійній основі. Серед них: 7 кандидатів юридичних наук та 3 доценти. На грудень 2010 року призначено черговий захист дисертації.

Всі дисертаційні дослідження проведені в рамках оперативно-розшукової спеціальності. З них 2 – за напрямком підготовки фахівців спеціалізації ОРД в СІТ:

1. "Використання комп'ютерних засобів для вирішення завдань оперативної розробки" – 2009 рік.
2. "Розкриття оперативними підрозділами ДСБЕЗ МВС України злочинів у сфері використання комп'ютерної інформації" – 2010 рік.

Науково-викладацький склад кафедри, який задіяно до підготовки курсантів спеціалізації, регулярно проходить із відривом від основної роботи місячне стажування у підрозділах по боротьбі з правопорушеннями у сфері інтелектуальної власності та комп'ютерних технологій ДСБЕЗ МВС України.

Навчально-методичне забезпечення спеціалізації представлено наступною документацією: програмами навчальних дисциплін; робочими навчальними програмами навчальних дисциплін кафедри; навчально-методичними матеріалами навчальних дисциплін кафедри; тематичними планами навчальних дисциплін; збірниками планів семінарських і практичних занять; програмами навчальної та позанавчальної практики та стажування курсантів; методичними матеріалами для курсантів з питань підготовки курсових та дипломних робіт; фондовими лекціями; методичними розробками, фабулами стандартних завдань та оперативно-тактичних навчань; макетами оперативно-розшукових справ та архівними справами оперативного обліку; завданнями з модульного контролю; дидактичними матеріалами (в тому числі спеціалізованими комп'ютерними програмами); тестовими завданнями для поточного контролю успішності курсантів (у паперовому та електронному вигляді); програмою та білетами державного екзамену. Навчально-методичне забезпечення підготовлено із дотриманням встановлених вимог.

Матеріально-технічне забезпечення кафедри відповідає сучасному рівню підготовки фахівців. У розпорядженні кафедри є спеціалізована лекційна зала, пристосована для проведення режимних занять, яку обладнано мультимедійним проектором, мультимедійним презентором, підсилювачем звуку з мікрофоном та акустичною системою, телевізорами, відеомагнітофоном та портативним комп'ютером. В аудиторіях, які використовуються кафедрою для проведення занять, встановлено 6 телевізорів, 2 відеомагнітофони, 3 DVD-програвачі, 3 кодоскопи.

Окрім того, на кафедрі функціонує спеціалізована аудиторія – комп'ютерний клас, який обладнано 16 комп'ютерами (15 комп'ютерів, 1 – сервер). Техніка із сучасними характеристиками надає можливість використовувати у навчальному процесі сучасні мультимедійні навчальні програми та роботу в мережі Інтернет.

Кафедра обладнана захищеним кабінетом та комп'ютеризованим робочим місцем для виконання режимних робіт з підготовки навчально-методичних і наукових матеріалів. Всього на балансі кафедри знаходиться 20 одиниць сучасної комп'ютерної техніки.

Кафедрою в рамках спеціалізації постійно проводяться тематичні науково-практичні заходи:

- 6–7 грудня 2002 року – Міжвузівська науково-практична конференція "Правове, кадрове та методичне забезпечення діяльності ОВС у боротьбі зі злочинністю у сфері інформаційних технологій";

- 30 жовтня 2003 року – Інноваційно-правовий захід – “Злочині у сфері інформаційних технологій”;
- 31 травня 2005 року – Науково-практичний семінар “Негласне отримання оперативної інформації з віддаленого комп’ютера”;
- 28 січня 2006 року – Науково-практичний семінар “Використання інформаційних технологій у боротьбі зі злочинністю”;
- 18–19 травня 2006 року – Міжнародна науково-практична конференція “Міжнародне співробітництво у боротьбі з комп’ютерною злочинністю: проблеми та шляхи їх розв’язання”;
- 25 травня 2007 року – Круглий стіл “Актуальні питання оперативно-розшукової діяльності”;
- 29 листопада 2007 року – круглий стіл “Актуальні проблеми діяльності Департаменту по боротьбі зі злочинами пов’язаними з торгівлею людьми МВС України”;
- 14 грудня 2007 року – Міжвузівська науково-практична конференція “Боротьба зі злочинами у сфері комп’ютерної інформації: проблеми та шляхи їх розв’язання”;
- 9 вересня 2008 року – Круглий стіл “Особливості розкриття злочинів в сучасних умовах”;
- 12 грудня 2008 року – Регіональний науково-практичний семінар “Взаємодія правоохоронних органів із провайдерами та операторами зв’язку в боротьбі з комп’ютерними злочинами”;
- 4 грудня 2009 року – Всеукраїнська науково-практична конференція “Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп’ютерних мережах та мережах електрозв’язку”;
- 12 листопада 2010 року заплановано проведення Всеукраїнської науково-практичної конференції “Протидія злочинності у сфері інтелектуальної власності та комп’ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи їх вирішення”.

За підсумками досліджень науково-викладацького складу кафедри у практичну діяльність, в тому числі на рівні Департаментів МВС України, за спеціалізацією було впроваджено 8 методичних та науково-практичних матеріалів:

1. Організаційно-тактичні основи діяльності оперативних підрозділів у сфері високих технологій.
2. Розкриття оперативними підрозділами ДСБЕЗ МВС України злочинів у сфері використання комп’ютерної інформації.
3. Використання комп’ютерних засобів для вирішення завдань оперативної розробки.

4. Проблемні питання розкриття оперативними підрозділами ДСБЕЗ МВС України злочинів у сфері використання комп'ютерної інформації.
5. Фіксація комп'ютерних слідів при розкритті злочинів.
6. Відновлення комп'ютерної інформації під час здійснення оперативно-розшукової діяльності.
7. Організація і тактика документування підрозділами ДСБЕЗ злочинів в комп'ютерних мережах та мережах електрозв'язку.
8. Особливості тактики документування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Між факультетом кримінальної міліції інституту та Департаментом ДСБЕЗ МВС України з 2005 року укладені угоди про співпрацю. В рамках реалізації угод з 2007 року кращі курсанти спеціалізації та ад'юнкти кафедри проходять у відділі Департаменту двохмісячне стажування.

З 2009 року в рамках угоди про співпрацю здійснюється взаємодія з Департаментом боротьби з кіберзлочинністю та торгівлею людьми МВС України. У 2010 році у відповідному відділі трьохмісячне стажування пройшов курсант-випускник спеціалізації та двохмісячне стажування проходить викладач кафедри. У практичну діяльність підрозділу впроваджені науково-практичні матеріали кафедри.

Наявне кадрове, навчально-методичне та матеріально-технічне забезпечення дозволяє здійснювати якісну підготовку на базі факультету кримінальної міліції Донецького юридичного інституту ЛДУВС імені Е.О. Дідоренка фахівців з протидії злочинам, пов'язаним із використанням комп'ютерних мереж, в тому числі протидії кіберзлочинності в банківській сфері.

О.Д. Довгань, *канд. юрид. наук, ст. науковий співробітник,*
директор Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України

ЕЛЕКТРОННИЙ ТЕРОРИЗМ ТА ЕЛЕКТРОННЕ ШПИГУНСТВО – СУЧАСНИЙ ВИКЛИК ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Одним із найбільш важливих питань сучасної світової громади є протидія тероризму, форми і методи якого набули значного розвитку на протязі останніх двох століть, коли достатньо гостро постають проблеми етнічного, релігійного, політичного та соціального характеру.

У загальному випадку, тероризм як вид злочинної діяльності, представляє собою дії по створенню передумов для реалізації ситуативних загроз благополуччю, життю та здоров'ю громадян, національній безпеці держави в політичній, економічній, військовій, соціальній та інших визначальних сферах, що мають за мету примушення суспільства та держави до прийняття рішень, які відповідають противоправним вимогам злочинних елементів.

Сьогодні, в умовах розвитку інформаційного суспільства, значного поширення інформаційно-телекомунікаційних технологій на рівні держави, суспільства та особи, особливої гостроти набувають питання комп'ютерної злочинності у контексті забезпечення національної безпеки держави.

Сучасний злочинний світ та різні організації противоправної спрямованості, мають досить широкі можливості для використання комп'ютерних технологій для реалізації злочинів, у тому числі і тих, що мають терористичний характер. При цьому є всі підстави для того, щоб вважати методи електронного тероризму не менш небезпечними за своїми наслідками, ніж загрози фізичного нападу на життєво важливі об'єкти.

Таким чином, доцільно звернути увагу на питання протидії електронному тероризму як одному із напрямів забезпечення інформаційної безпеки держави.

Національні інформаційно-телекомунікаційні системи (надалі – ІТС) є одними із приоритетних об'єктів захисту від загроз електронного тероризму, оскільки порушення заходів їх інформаційної безпеки може призвести до безпрецедентних наслідків щодо життєво важливих складових безпеки особи, суспільства та держави.

Так, наприклад, не треба переконувати учасників конференції у тому, що безпека інформаційно-телекомунікаційних технологій банківської системи України до потенційних загроз електронного тероризму, безпосередньо впливає на стан національної безпеки держави в економічній сфері.

Крім того, не можна оминути увагою можливі комп'ютерні злочини, що спрямовані на системи автоматизованого управління транспортними засобами, об'єктами енергетики та комунікаціями, що мають стратегічне призначення. Наприклад, атаки на автоматизовані системи енергопостачання, управління польотами та рухом наземного транспорту та багато інших.

Питання комп'ютерної злочинності представляють також вагомий інтерес і в завданнях контррозвідувальної діяльності. Оскільки в су-

часних умовах активного впровадження систем електронного документообігу, комп'ютерна розвідка та електронне ("кібер") озброєння вважається одним із найбільш ефективних напрямів розвідувально-підривної діяльності. Крім того, розвиток сучасних методів комп'ютерної стеганографії (методів приховування факту зберігання або передачі інформації в комп'ютерних мережах), визначає абсолютно нові можливості в організації агентурної роботи та підготовки противоправних діянь, які були недоступними ще 10–15 років назад.

Більш того, технології ІТС, насамперед мережі Інтернет, можуть використовуватися для реалізації маніпулятивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан громадян з метою формування у них стану тривоги та паніки, очікування насильницьких нападів тощо.

Підсумовуючи сказане, слід зазначити, що завдання протидії електронному тероризму та електронному шпигунству, як різновиду комп'ютерної злочинності, доцільно розглядати в рамках комплексного підходу до забезпечення інформаційної безпеки держави, що передбачає:

- заходи організаційно-правового, технічного та криптографічного захисту інформаційних ресурсів в ІТС;
- заходи захисту інформаційного простору ІТС від загроз застосування інформаційно-психологічних атак;
- контррозвідувального забезпечення процесу захисту інформаційних ресурсів та інформаційного простору в ІТС у контексті оперативно-розшукових та оперативно-технічних заходів.

Враховуючи факт особливого значення інформаційно-телекомунікаційних технологій банківської системи України в забезпеченні інформаційної безпеки держави, вважається актуальним завдання координації зусиль правоохоронних органів, спеціальних служб та Національного банку України з питань протидії комп'ютерній злочинності, у тому числі і в напрямах протидії електронному тероризму та електронному шпигунству в банківській сфері.

Література

1. Інтернет-ресурс (www.crime-research.org).
2. Інформаційна безпека: наукові здобутки, ідеї, рекомендації: Збірник матеріалів. – К.: НКЦ СБ України, 2008. – 288 с.
3. Актуальні проблеми забезпечення інформаційної безпеки держави: зб. Матеріалів наук.-практ. конф., Київ, 20 березня 2009 р./ НА СБ України, Ін-т захисту інформації з обмеженим доступом. – К.: Наук.-вид. відділ НА СБ України, 2009 р. – 200 с.

Л.Л. Тимченко, *канд. юрид. наук,*
головний оперуповноважений інспектор
Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України

ПРОТИДІЯ ЗЛОЧИНАМ, ЩО ВЧИНЯЮТЬСЯ У СФЕРІ ВИКОРИСТАННЯ ПЛАТІЖНИХ КАРТОК, ОРГАНАМИ ВНУТРІШНІХ СПРАВ: СТАН, ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Пасивність вітчизняних банків у розвитку карткових технологій призвела до різкого зростання шахрайств з платіжними картками. За даними Національного банку, кількість шахрайських операцій із використанням платіжних карток, емітованих українськими банками, у 2009 році зросла порівняно із 2008 роком в 6,5 разів до 39,3 тисяч випадків [1]. Сьогодні вже не секрет, що банки та платіжні системи традиційно намагаються укривати реальні обсяги карткових крадіжок, з метою збереження довіри клієнтів до платіжних карток. Тому, як зазначають фахівці у сфері боротьби зі злочинами що вчиняються із викоритстанням платіжних карток, і така статистика є значно заниженою. Істинний обсяг шахрайських операцій з платіжними картками сьогодні відповідально оцінити ніхто не береться. Та все ж статистика НБУ чітко відображає негативну тенденцію. Така ситуація в основному пояснюється тим, що банки-члени міжнародних платіжних систем не приділяють істотної уваги захисту інформації, а також продовжують емітувати платіжні картки з магнітною стрічкою, які є вкрай незахищеними. Національний банк України зобов'язав банки прискорити перехід на використання платіжних карток з чипами, забезпечити встановлення добових лімітів на суми і кількість операцій по отриманню готівки як на території України, так і за її межами [2].

Ріст злочинності із використанням платіжних карток був прогнозованим. В умовах фінансової кризи банкіри практично перестали розвивати цей напрямок, зосередивши зусилля на рятування своїх активів. Кількість активних платіжних карток (тобто карток, по яким реально проводились операції по оплаті товарів чи зняття готівки в банкоматах) в Україні в 2009 році скоротилось на 24,6 % – до 29,1 млн. шт. При цьому до початку 2010 року кількість карток із магнітною стрічкою складала 93 % від загальної кількості активних платіжних карток. Списувати усі проблеми на фінансову кризу зараз вже стало майже модно, однак істинні причини ситуації що склалася на ринку платіжних карток, зароджувались ще у докризовий період, коли у банків були засоби на розвиток бізнесу, а у клієнтів сучасні технології викликали живий інтерес. Міжнародні платіжні системи у рамках боротьби із шахрайством прийн-

яли рішення про перехід з магнітних карток на чипові ще в 2005 році. Формально пластик із магнітною стрічкою може використовуватись паралельно із чиповими картками досить довгий період. Однак вже у 2005 році у країнах Західної Європи було запроваджено нові правила безпеки при проведенні операцій з картками. Зокрема, вступило в силу правило про "перенесення відповідальності" – тепер за всі втрати від шахрайських операцій відповідає та сторона, яка не завершила перехід на чип. В результаті власники багатьох магазинів та ресторанів Західної Європи, остерігаючись шахраїв, відмовились обслуговувати власників традиційних магнітних карток, що і змусило банкірів вкладати серйозні кошти і швидко перейти на нові картки із чипом. Процес переходу зайняв у європейських фінансових установ два-три роки. При цьому відбувалась не тільки заміна карток, але і повне переобладнання банкоматних і термінальних мереж. Українські ж банки весь цей час лише приглядались до нових технологій, не відчуваючи достатніх стимулів для їх розвитку. Вітчизняні банкіри продовжували емітувати картки із магнітною стрічкою, обмежившись окремими пробними проектами, в основному по випуску комбінованих (із стрічкою та чипом) платіжних карток. Як наслідок, час був безповоротньо втрачений, а криза лише загострила ситуацію. Шахраї, що залишали європейські країни, змушені були звернути свою увагу на менш технологічні банківські ринкиі, перш за все, на Україну, де утворилась унікальна ситуація: велика кількість випущених карток на фоні підвищеної вразливості як самих карток, так і мереж передачі даних.

Банкіри в більшості своїй погоджуються із НБУ, що впровадження чипових карток може дозволити максимально захистити власників карток і знизити ризики шахрайства до мінімуму. Картку, що має чип, часто називають смарт-карткою (від англ. – smart – інтелектуальний). Основною особливістю карток із чипом або смарт-карток є те, що замість (або окрім) магнітної стрічки вони мають інтегральну мікросхему. Чип-модулі містять мікроконтролер, постійну пам'ять та пам'ять із можливістю перезапису. Це дозволяє зберігати на карточці досить великий обсяг інформації та, що ще більш важливо, при необхідності її змінювати. В результаті зазначених переваг рівень безпеки у смарт-карток на порядок вищий. Чипову картку нині практично не можливо підробити. Крім того, смарт-картка дозволяє проводити перевірку клієнта без відправлення запиту до фінустанови, а в деяких випадках і здійснювати транзакцію на багато бистріше (немає необхідності чекати відповідь із банку). Чип на картці не піддається дії магнітних полей, не боїться вологи, легких подряпин, і таким чином є більш надійним. Однак головна причина, по якій банки почали випускати ці картки, –

високий рівень захисту данних клієнта та його грошових коштів на рахунку. Умови перевірки PIN-коду для таких карток суттєво відрізняються від процедури перевірки PIN-коду карток із магнітною стрічкою. Крім того, чип має великий криптозахист порівняно із магнітною стрічкою, він складніший у виготовленні. Усе це значно ускладнює підробку таких карток, та робить їх виготовлення в кустарних умовах економічно не вигідним та майже неможливим. Транзакція за допомогою каркти із магнітною стрічкою використовує завжди однакові ідентифікаційні дані, що передаються у банк. Тому їх можливо перехватити та виготовити підроблену платіжну картку. Чипова ж картка працює інакше: кожна транзакція підтверджується сформованим спеціально для неї кодом, та для наступної транзакції потребує новий код. Тому використовувати дані транзакцій що вже відбулись безглуздо, а зробити дублікат чипу практично не можливо. Як результат – нині у всьому світі не зафіксовано жодного випадку шахрайства із смарт-картками.

Проблеми розвитку банківських технологій в наших умовах являють собою замкнуте коло. У банкірів та торговців відсутня мотивація до встановлення банкоматів і терміналів для карток, що не отримали визнання покупців, в той час, як це визнання виникає лише в тому випадку, коли люди зможуть розраховуватись більш технологічними картками при оплаті товарів і послуг та безперешкодно отримувати кошти з банкоматів. Таким чином, оцінюючи перспективи карткових технологій, можливо стверджувати що в Україні нові проекти міжнародних платіжних систем з'являться не скоро. І не тільки по причині фінансової кризи та бажання економити, а тому що більшість "прогресивних" рішень без зобов'язання або активного просування в нашій країні частіше всього приречені на невдачу.

Підсумовуючи зазначене вище, необхідно додати, що за даними МВС України кількість виявлених злочинів у сфері використання платіжних карток незмінно зростає із року в рік. Так, якщо у 2003 році було виявлено 65 злочинів вказаної категорії, то у 2009 вже 233.

Шахраї намагаються розробляти все нові схеми вчинення злочинів із використанням платіжних карток. Як зазначають фахівці, окрім використання так званих "скіммерів", злочинці виготовляють та активно використовують так звані "шиммери" – тонкі картки, які розміщують в отвір для прийнятя справжніх карток. Даний пристрій дозволяє зчитати інформацію з магнітної стрічки платіжної картки [3]. На території України такі факти поки що не зареєстровані, але це не означає що такі пристрої не використовуються.

Незмінною є статистика виявлення на території України скіммінгових пристроїв. В 2007 році в органах внутрушніх було зареєстровано

перший випадок виявлення так званої "накладки" на банкомат. У 2008 – 9, 2009 – 11.

Існує стандартний перелік застережень для користувачів платіжною карткою:

- не передавати платіжну картку стороннім особам;
- PIN-код зберігати окремо від картки. Не записувати його на картку та не носити в гаманці;
- підключити послугу SMS-banking;
- звертати увагу на клавіатуру бункомату та картоприймач. В разі виявлення сторонніх предметів негайно телефонувати в банк;
- переписати в свій мобільний телефон номер телефону цілодобової банківської підтримки;
- по можливості прикривати долонею клавіатуру при наборі PIN-коду;
- використовувати банкомати що розташовані в людних, добре освітлених місцях.

Література

1. http://cripo.com.ua/?sect_id=4$&aid=92658.
2. http://cripo.com.ua/?sect_id=10$&aid=98859.
3. http://dengi.ua/news/65747_Novyj_sposob_krazhi_deneg_s_bankovkih_kart.html.

А.Г. Чубенко, *канд. юрид. наук, ст. науковий співробітник, докторант кафедри економіко-правових дисциплін Національної академії внутрішніх справ*

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ ЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ МЕРЕЖ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Забезпечення захисту населення, об'єктів економіки, національного надбання від надзвичайних ситуацій техногенного, природного або іншого характеру, що здійснюється за рахунок функціонування єдиної системи цивільного захисту, визначається Законом України "Про основи національної безпеки" як один з пріоритетів національних інтересів. Відповідно до ст. 7 цього Закону до загроз національній безпеці України в екологічній сфері віднесено, зокрема, небезпеку техногенного, у тому числі ядерного та біологічного, тероризму, а у інформаційній сфері – комп'ютерна злочинність та комп'ютерний тероризм, розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави, намагання маніпулювати суспільною свідомістю,

зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [1].

Кіберзлочинність перетворюється на реальну загрозу екологічній та інформаційній безпеці у сфері цивільного захисту. Адже науково-технічна революція, що розпочалася у XX столітті й триває по цей час, призвела до значного зростання матеріальних і духовних можливостей людства – як творчих, так і руйнівних. Недбале використання цих можливостей призводить до трагічних наслідків. Нині світове суспільство приділяє значну увагу гострим екологічним проблемам. Сучасна цивілізація – це цивілізація постіндустріальна, це високі технології і інформаційне суспільство. Все це буде визначати майбутнє суспільства [2].

На цей час питання забезпечення інформаційної безпеки у сфері цивільного захисту врегульовані нормами Конституції України, Законів України від 19 червня 2003 року № 964 "Про основи національної безпеки", від 3 лютого 1993 року № 2974 "Про цивільну оборону України", від 8 червня 2000 року № 1809 "Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру", від 24 червня 2004 року № 1859 "Про правові засади цивільного захисту", а також Законів "Про інформацію", "Про телекомунікації", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про пожежну безпеку", указу Президента України: "Про рішення Ради національної безпеки і оборони України "Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин", "Про рішення Ради національної безпеки і оборони від 31 жовтня 2001 р. "Про заходи щодо вдосконалення державної політики та забезпечення інформаційної безпеки України". Окремі заходи визначені Президентом України в указах: "Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень" від 14 липня 2000 р. № 891; "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" від 31 липня 2000 р. № 928/2000; "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних" від 24 вересня 2001 р. № 891/2001 та інших.

Питання інформаційного забезпечення функціонування єдиної державної системи цивільного захисту (далі – ЄДСЦЗ) та її елементів може розглядатися в двох аспектах залежно від напряму руху інформаційних потоків. З одного боку, мова іде про інформаційне та інше забезпечення життєдіяльності складових (структурних елементів) системи з метою підготовки сил та засобів суб'єктів системи до їх оперативного

застосування згідно з призначенням, реалізації функції прогнозування, виявлення та оцінки можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву. З іншого боку інформаційне забезпечення діяльності ЄДСЦЗ передбачає функціонування дієвої системи інформування та оповіщення населення у разі виникнення надзвичайних ситуацій та системи екстреної допомоги населенню за єдиним телефонним номером.

Враховуючи, що до складу ЄДСЦЗ входять органи управління, сили і засоби оперативного реагування, в першу чергу таких центральних органів виконавчої влади, як МНС, МВС, МОЗ, Мінтрансзв'язку, Мінпаливенерго, СБУ, ДССЗІ, їх відомчі телекомунікаційні мережі повинні становити основу системи зв'язку та оповіщення ЄДСЦЗНТ і технічно забезпечувати роботу органів управління ЄДСЦЗ на загальнодержавному, регіональному та місцевому рівнях [2].

Злочини, які вчиняються із використанням комп'ютерних мереж є реальною загрозою нормальному функціонуванню єдиної системи зв'язку та оповіщення. Зокрема, це стосується таких передбачених Кримінальним кодексом України видів комп'ютерних злочинів (кіберзлочинів), як "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку" (мова іде про несанкціоноване втручання, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, що може порушити нормальне функціонування єдиної системи зв'язку та оповіщення про надзвичайні ситуації), "Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації" (склад злочину передбачений ст. 361-2 Кримінального кодексу), "Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку" (ст. 363-1 КК) [3].

Внаслідок вчинення зазначених злочинів можке бути порушена робота систем автоматизованого контролю за станом радіаційних і хімічних підприємств, інших об'єктів підвищеної небезпеки і оповіщення про загрозу та виникнення надзвичайних ситуацій.

Створення системи зв'язку та оповіщення єдиної державної системи цивільного захисту шляхом використання сучасних технологій дає можливість прогнозувати досягнення таких показників системи, як підвищення оперативності дій щодо запобігання та ліквідації нас-

лідків надзвичайних ситуацій шляхом скорочення часу для передачі сигналів управління; здійснення захисту інформації, що циркулює між об'єктами системи, що дозволить класифікувати інформацію та надавати доступ до її використання тільки визначеним користувачам; мінімального зменшення впливу помилок, пов'язаних із людським фактором, шляхом використання автоматизації організаційних і технічних процесів та використанням автоматичного контролю за діями персоналу; надання можливості для збору та публікації інформації через мережу інтернет; створення інтерфейсів для взаємного обміну інформацією із заінтересованими сторонами у межах міждержавної взаємодії у вирішенні завдань щодо запобігання та ліквідації наслідків надзвичайних ситуацій; надання сервісних функцій з доступу до інформації, довідкових баз даних, картографічних, статистичних даних тощо, що сприятиме скороченню часу приймання рішення під час вирішення завдань, пов'язаних із запобіганням та ліквідацією наслідків надзвичайних ситуацій [2].

Висновки. Враховуючи очікуваний позитивний ефект від створення системи зв'язку та оповіщення та з метою забезпечення протидії злочинам, які вчиняються з використанням комп'ютерних мереж, пропонуємо передбачити у ст. 361 Кримінального кодексу України частину третю з метою посилення відповідальності за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які входять до єдиної державної системи зв'язку та оповіщення єдиної державної системи цивільного захисту населення і територій. Крім того, для створення системи зв'язку та оповіщення необхідно розробити ряд нормативно-правових актів стосовно взаємодії з відомчими та іншими мережами, що залучаються; взаємодії мережі, яка створюється з телекомунікаційною мережею загального користування та забезпечення функціонування мережі (фінансове та матеріально-технічне) у повсякденних та надзвичайних умовах.

Література

1. Про основи національної безпеки України: Закон України від 19.06.2003 року № 964 // Відомості Верховної Ради України (ВВР), 2003, № 39, ст. 351.
2. Концепція Державної цільової програми створення системи зв'язку та оповіщення єдиної державної системи цивільного захисту населення і територій до 2012 року // http://www.mns.gov.ua/content/public_discus.html.
3. Кримінальний кодекс України // Офіційний вісник України від 08.06.2001 – 2001 р., № 21, стор. 1, стаття 920, код акту 18825/2001.
4. Про інформацію: Закон України від 2.10.1992 р. № 2657 // Відомості Верховної Ради України від 01.12.1992 – 1992 р., № 48, стаття 650.

5. Кодекс України Про цивільний захист: Проект // http://www.mns.gov.ua/content/reg_acts.html.

С.В. Мельник, *канд. техн. наук, доц. спеціальної кафедри*
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України

АКТУАЛЬНІ НАПРЯМИ ПРОТИДІЇ КОМП'ЮТЕРНІЙ ЗЛОЧИННОСТІ У БАНКІВСЬКІЙ СФЕРІ В КОНТЕКСТІ КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАХИСТУ ІНФОРМАЦІЇ

Як ми всі з Вами розуміємо, комп'ютерна злочинність для України вже не є екзотикою, а одним із найбільш небезпечних викликів інформаційній безпеці держави. Процеси бурхливого розвитку та впровадження новітніх інформаційних, комп'ютерних та телекомунікаційних технології дають значний поштовх для розвитку практично усіх сфер державного та суспільного життя, але і одночасно стимулюють розвиток нових форм злочинності, що у більшості випадків мають на меті неправомірне збагачення шляхом несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем.

Мова йде про крадіжки інформації, програм і так званого "комп'ютерного ресурсу", традиційні економічні злочини, що вчиняються за допомогою технологічних можливостей сучасних комп'ютерних і телекомунікаційних мереж. Найбільш поширеними комп'ютерними злочинами є шахрайства з кредитними картками, злочини у сфері телекомунікації (шахрайства з оплатою міжнародних телефонних розмов), несанкціонований доступ в системи електронних платежів, економічне шпигунство та багато інших.

На підставі результатів аналізу фахової літератури можна стверджувати, що на сьогоднішній день має місце певна дискусія відносно трактування самого визначення "комп'ютерної злочинності", яке базується на класичних правових підходах до визначеннях злочину як соціального явища, з урахуванням ознак предмету злочину і знарядь його вчинення. Однак фахівці технічного профілю не бачать у цьому питанні ніякої проблеми і вважають очевидним, що комп'ютерний злочин – це несанкціоноване порушення конфіденційності, цілісності, авторства та доступності інформації в інформаційно-телекомунікаційних системах, що здійснюється в рамках їх технологічних функцій. Незалежно від того, чи ставить злочинець за мету неправомірне збагачення, досягнення переваг у конкурентній боротьбі, або ж мова йде про електронну розвідку, електронний тероризм та електронні диверсії. Різниця полягає лише у можливих наслідках цієї неправомірної діяльно-

сті, технологічна ж сторона є однаковою – використання технічних недоліків механізмів безпеки сучасних інформаційно-телекомунікаційних систем та людського фактору, що додатково впливає на рівень їх адекватності широкому спектру загроз безпеці інформації.

Окремою категорією правопорушень є мабуть інформаційно-психологічні впливи на свідомість, психологічний та психічний стан громадян з використанням технологічних можливостей сучасних інформаційно-телекомунікаційних систем. Крім того, доцільно також звернути увагу на технологічні можливості побудови прихованих і захищених каналів зв'язку в інформаційно-телекомунікаційних системах, що можуть бути використані для організації противоправної діяльності, у тому числі і терористичного характеру.

У загальному випадку, заходи протидії комп'ютерній злочинності можна розділити на організаційно-правову, соціальну та технічну частину. При цьому технічна частина розділяється на заходи захисту інформації в інформаційно-телекомунікаційних системах та заходи по розслідуванню комп'ютерних злочинів.

В рамках доповіді буде зосереджена увага лише на питаннях превентивних заходів протидії комп'ютерній злочинності, що стосуються організації комплексного захисту інформації.

Далі, через призму основних понять інформаційної безпеки у сфері інформаційно-телекомунікаційних технологій, розглянемо найбільш важливі проблемні питання захисту систем електронних банківських платежів, які є одним із найпривабливіших об'єктів комп'ютерних злочинів.

Так, під безпекою інформації, як технічної складової поняття інформаційної безпеки, прийнято розуміти стан захищеності інформації від загроз несанкціонованого витоку (розголошення), нав'язування (порушення цілісності та/або авторства), знищення та блокування під час її виготовлення, зберігання, обробки, передачі та знищення.

В свою чергу, забезпечення безпеки інформації – це безперервний процес, який представляє собою систематичний контроль за станом захищеності інформації, виявлення вузьких місць у системі захисту, обґрунтування та реалізацію найбільш раціональних шляхів удосконалення і розвитку системи захисту.

Основними заходами забезпечення безпеки інформації є методи технічного та криптографічного захисту інформації, що включають в себе як технічну, так і організаційно-технічну складову. Додатково, в залежності від моделі загроз, використовуються також методи біометричної автентифікації, голографічного захисту носіїв інформації та інженерно-технічного контролю об'єктів інформаційної діяльності.

Інфраструктура електронних платіжних систем України, як об'єкту захисту, складається з наступних систем.

Система електронних платежів Національного банку України (СЕП) – державна система міжбанківських розрахунків.

Система "клієнт-банк" (on-line/off-line) – система дистанційного обслуговування поточних рахунків клієнтів комерційними банками.

Платіжна система банківських карт – система обслуговування особистих рахунків клієнтів комерційних банків через банкоматні мережі.

Електронні гроші – технології електронного гаманця та електронного чеку, наприклад, національна система масових електронних платежів (НСМЭП).

Оцінюючи загальний рівень захищеності систем електронних платежів необхідно враховувати:

- властивості криптографічних алгоритмів і протоколів;
- технічні канали несанкціонованого доступу до таємних ключів криптографічних перетворень;
- можливості несанкціонованої модифікації технічних рішень із реалізації криптографічних алгоритмів і протоколів;
- технічні канали витоку інформації про ключі за рахунок побічних електромагнітних випромінювань та наведень;
- можливі помилки або навмисні дії користувачів систем електронних платежів та працівників банку, що можуть призвести до порушення безпеки інформації;
- можливі технічні збої у роботі систем електронних платежів, що можуть також призвести до порушення безпеки інформації.

Таким чином, достатній рівень захисту систем електронних платежів може бути забезпеченим лише за умови використання комплексного підходу до захисту інформації в інформаційно-телекомунікаційних системах, включаючи і механізм страхування інформаційних ризиків.

Комплексний підхід до захисту інформації – це взаємопов'язана сукупність методів усіх видів захисту інформації, що обираються в залежності від моделі загроз для конкретного об'єкта інформаційної діяльності. В основі комплексного підходу до захисту інформації лежать два базових поняття у сфері технічного захисту інформації, а саме "захист від несанкціонованого доступу до інформації в комп'ютерних системах" та "захист інформації від витоку технічними каналами".

Міжнародна статистика випадків розкрадання коштів у системах електронних платежів свідчить про значну кількість атак на системи типу "клієнт-банк" та "електронні гроші". У загальному випадку ці атаки спрямовані на викрадання файлів із ключами, паролями доступу до ключів, паролями автентифікації, модифікацію відкритої інформації

перед запуском засобів криптографічного захисту інформації (надалі – КЗІ) або самих цих засобів, що відбуваються за рахунок факту недбалості клієнтів системи, які ігнорують елементарні запобіжні заходи безпеки.

Проблемою є відсутність діючого механізму забезпечення комплексного захисту інформації на клієнтських місцях зазначених систем.

У якості основних шляхів вирішення цієї проблеми можна розглянути наступні рішення.

1. Використання захищених носіїв ключової інформації для програмних засобів КЗІ з функціями забезпечення цілісності виконавчого файлу.
2. Використання апаратних засобів КЗІ, у яких виключаються всі операції із секретними ключами на комп'ютері клієнта.
3. Інформування користувачів систем про правила безпечного використання комп'ютера і засобів КЗІ. Мотивування клієнтів банку до використання захищених комп'ютерів та фіксованої IP-адреси для роботи системи по захищеному каналу.
4. Використання механізмів страхування ризиків.

У загальному випадку, до актуальних завдань забезпечення безпеки електронних платежів можна також віднести.

1. Розробку адекватних до реальних загроз методик оцінювання страхових ризиків порушення безпеки електронних платіжних систем.
2. Розробку "економічно привабливих" алгоритмічних, технічних і організаційно-технічних рішень для систем "клієнт-банк" і систем "електронних грошей", що реалізують комплексний підхід до захисту та зменшують ступінь впливу людського фактору на рівень безпеки платіжної системи.
3. Забезпечення діючої взаємодії банківської системи і правоохоронних органів України в завданнях боротьби з кіберзлочинністю.

Та інші.

Література

1. Інтернет ресурс (www.crime-research.ru).
2. І. Стельник, С. Мельник. Актуальные вопросы нормативно-правового регулирования в области криптографической защиты информации. Тезисы доклада XIII международной научно-практической конференции "Безопасность информации в информационно-телекоммуникационных системах", 18–21 мая 2010 г.

Ю.О. Тараненко, *канд. екон. наук, доц.,*
начальник кафедри економіко-правових дисциплін,
Н.А. Берлач, *канд. екон. наук, доц. кафедри економіко-правових дисциплін*
Національна академія внутрішніх справ

ЗЛОЧИННІСТЬ У БАНКІВСЬКІЙ СФЕРІ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Для нормального функціонування економіки необхідна надійна, стабільна і розвинена банківська система, при якій банки будуть здійснювати платежі, вчасно надавати своїм клієнтам кредити, послуги з операцій з цінними паперами тощо. Саме належне здійснення банківської діяльність – залучення у вклади грошових коштів фізичних і юридичних осіб та розміщення зазначених коштів від свого імені, на власних умовах та на власний ризик, відкриття і ведення банківських рахунків фізичних та юридичних осіб забезпечує використання банків як координуючих елементів у всій фінансовій системі нашої держави [1].

Банківська система України складається з Національного банку України та комерційних банків, що створені і діють на території України відповідно до положень закону України "Про банки і банківську діяльність" від 7 грудня 2000 року [2].

Разом з тим, останнім часом, внасліок функціонування кризових явищ в економіці України, зросла кількість правопорушень в банківській сфері. На нашу думку, при загостренні даних явищ, а особливо – у межах всієї держави, призвести до виникнення загроз національній безпеці України.

За умов нинішньої нестабільності у суспільстві та економічної кризи, на фоні послаблення реального впливу держави на макро- і мікрорівнях, доларизації грошового обігу, посилення структурних деформацій в економіці відбувається значне зростання кількості вчинених корисливих злочинів. Значною мірою вражена кримінальними правопорушеннями кредитно-фінансова та банківська сфера, в яких кількість злочинів постійно збільшується. Викрито чимало фактів незаконного отримання й нецільового використання пільгових кредитів, переливу капіталів у "тіньову" економіку і зарубіжні банки, "відмивання" грошей, здобутих злочинним шляхом.

За своїм змістом акцент зловживань у банківських установах все помітніше переміщується від правопорушень, пов'язаних з кредитуванням, до відтоку грошової маси за кордон, "відмивання брудних" коштів шляхом акціонування підприємств, вкладання їх в нерухомість, укладання фіктивних угод, повернення незаконно вивезених грошей в

якості інвестицій. Все активніше організована злочинність проявляє інтерес до операцій з цінними паперами [3].

Розширення мережі кореспондентських відносин українських банків із зарубіжними банківськими установами та включення до системи електронних міжбанківських міжнародних розрахунків залишаються майже не захищеними перед можливостями їх використання організованими злочинними угрупованнями для налагодження функціонування стійких каналів незаконного витоку за кордон валютних коштів через систему лоро-рахунків. Сформовано мережу фіктивних комерційних структур, які займаються конвертацією безготівкових коштів юридичних осіб різних форм власності у готівкову валюту, створено механізм переказу резидентами України валютних коштів на неконтрольовані державою рахунки у закордонних банках під виглядом оплати імпортних контрактів [4].

У м. Києві резонансною справою стала ліквідація у 2008 р. найбільшого у столиці конвертаційного центру. До його послуг вдавалися понад 3 тис. комерційних організацій і державних установ.

Через злочинну діяльність у фінансово-кредитній і банківській сферах економіка України втратила значну суму коштів, які знаходяться зараз за межами держави. Валютні цінності, котрі незаконно переведені за межі України, обчислюються мільярдами доларів; спроби повернути їх в Україну залишаються малоефективними.

Департаментом Державної служби боротьби з економічною злочинністю МВС України впродовж восьми місяців 2009 року у сфері банківської діяльності викрито 3 тис. 492 злочини, у тому числі безпосередньо у банках – 1 тис. 425 злочинів.

Про це УНІАН повідомили у Департаменті зв’язків з громадськістю МВС України.

За даними правоохоронців, кожен шостий викритий злочин зі збитками понад 100 тис. грн. Крім того, порушено 90 кримінальних справ, де збитки перевищують1 млн. грн.

За кримінальними справами на сьогодні уже відшкодовано 144,3 млн. грн., з яких згідно з постановами слідчих органів та суду накладено арешт на майно в сумі 89,4 млн. грн.

Водночас за виявленими злочинами до відповідальності притягнуто 574 осіб, з яких 74 керівники філій та відділень банківських установ, 128 інших службових осіб банків та 239 осіб, що вчинили злочини у складі груп.

Дану ситуацію цілком можна класифікувати як загрозу національній безпеці або явища і чинники, що створюють небезпеку життєво важливим національним інтересам України [5].

Згідно положень Закону України “Про основи національної безпеки України”, як шляхи подолання загроз національній безпеці в економічній сфері виділяють:

- забезпечення умов для сталого економічного зростання та підвищення конкурентоспроможності національної економіки;
- прискорення прогресивних структурних та інституціональних змін в економіці, поліпшення інвестиційного клімату, підвищення ефективності інвестиційних процесів; стимулювання випереджувального розвитку наукоємних високотехнологічних виробництв;
- вдосконалення антимонопольної політики; створення ефективного механізму державного регулювання природних монополій;
- подолання “тінізації” економіки через реформування податкової системи, оздоровлення фінансово-кредитної сфери та припинення відпливу капіталів за кордон, зменшення позабанківського обігу грошової маси;
- забезпечення збалансованого розвитку бюджетної сфери, внутрішньої і зовнішньої захищеності національної валюти, її стабільності, захисту інтересів вкладників, фінансового ринку;
- здійснення виваженої політики внутрішніх та зовнішніх запозичень;
- забезпечення енергетичної безпеки на основі сталого функціонування і розвитку паливно-енергетичного комплексу, в тому числі послідовного і активного проведення політики енергозбереження та диверсифікації джерел енергозабезпечення;
- забезпечення продовольчої безпеки;
- захист внутрішнього ринку від недоброякісного імпорту – поставок продукції, яка може завдавати шкоди національним виробникам, здоров’ю людей та навколишньому природному середовищу;
- посилення участі України у міжнародному поділі праці, розвиток експортного потенціалу високотехнологічної продукції, поглиблення інтеграції у європейську і світову економічну систему та активізація участі в міжнародних економічних і фінансових організаціях [6].

Як бачимо, в даному переліку відсутні положення, що передбачають активні дії щодо регулювання банківської системи з метою уникнення виникнення кризових явищ у всій економіці України.

Попри це, у Кримінальному Кодексі України передбачено цілий ряд статей стосуються саме банківської діяльності, зокрема:

Стаття 199. Виготовлення, зберігання, придбання, перевезення, пересилання, ввезення в Україну з метою збуту або збут підроблених грошей, державних цінних паперів чи білетів державної лотереї.

Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення.

Стаття 202. Порушення порядку зайняття господарської та банківською діяльністю.

Стаття 208. Незаконне відкриття або використання за межами України валютних рахунків.

Стаття 209. Легалізація (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом.

Стаття 218. Фіктивне банкрутство.

Стаття 219. Доведення до банкрутства.

Стаття 220. Приховування стійкої фінансової неспроможності.

Стаття 221. Незаконні дії у разі банкрутства.

Стаття 222. Шахрайство з фінансовими ресурсами [7].

Таким чином, здійснення злочинів у сфері банківської діяльності набуває такого значного рівня суспільної небезпечності завдяки глибокій інтеграції банківських установ у економічну систему. Попри значні вигоди, що приносить суспільству розвинена банківська сфера, наявний також широкий перелік загроз для національної безпеки, що зумовлено поширенням банківської злочинності. Саме тому, на нашу думку, враховуючи сьогоднішню ситуацію в аналізованій сфері, а також досить детальне регулювання даної сфери суспільних відносин Кримінальним Кодексом України необхідним є включення злочинів у банківській сфері до переліку загроз національної безпеки.

Література

1. Петренко Павло. Поняття та класифікація злочинів у банківській сфері // Юридичний журнал : аналітичні матеріали, коментарі, судова практика / МОН України; НПУ ім. Драгоманова; Ін-т політології та ін. – Київ, 2010. – № 3 (93). – С. 47–49.
2. Про банки і банківську діяльність: Закон України від 7 грудня 2000 року № 2121-III // Відомості Верховної Ради України від 09.02.2001 – 2001 р., № 5, стаття 30.
3. Виступ Президента України на Розширеному засіданні Координаційного комітету по боротьбі з корупцією і організованою злочинністю при Президентові України 14 грудня 1999 р. // Крок. – 2000. – січ. – № 2.
4. Про протидію “відмиванню” коштів та майна, отриманих злочинним шляхом // Інформаційні матеріали семінару. – К: Міністерство юстиції України, Посольство США. – 1999.
5. Звіт МВС про викриття злочинів у банківській сфері // [Електронний ресурс] – Режим доступу: http://www.unian.net/ukr/news/news-337025.html.
6. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України від 26.09.2003 – 2003 р., № 39, стаття 351.

7. Кримінальний кодекс України: від 05.04.2001 № 2341-III // Відомості Верховної Ради України від 29.06.2001 – 2001 р., № 25, стаття 131.

І.О. Воронов, *канд. юрид. наук,*
ст. науковий співробітник відділу з організації наукової роботи
Одеського державного університету внутрішніх справ

ПРОТИДІЯ ЗЛОЧИННОСТІ У СФЕРІ ВИСОКИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Процес розбудови правової держави в Україні безпосередньо пов'язаний з додержанням та належною реалізацією гарантованих прав і свобод людини, зокрема, їх право на інформацію. Саме тому, одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на неухильний розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій власний потенціал, сприяючи суспільному і особистому розвитку та підвищуючи якість життя.

Становлення в Україні інформаційного суспільства неможливе без широкого використання в усіх сферах суспільного життя високих інформаційних технологій, усвідомлення ролі інформаційних ресурсів, сприяння масовому доступу громадян до глобальної мережі Інтернет.

Високі інформаційні технології мають величезний потенціал, виступають одним з найбільш важливих факторів, що впливають на формування сучасного суспільства, оскільки практично стали життєво важливим стимулом розвитку світової економіки, дають можливість більш ефективно й творчо вирішувати економічні та соціальні проблеми. Унаслідок цього невпинно вдосконалюються існуючі або створюються нові апаратно-програмні засоби обробки інформації, підвищується швидкість передачі даних, з'являються нові види каналів зв'язку, виникають раніше невідомі послуги.

Усе це в сукупності виступає підґрунтям для вчинення злочинів у сфері високих інформаційних технологій, які складаються з таких видів кримінальних діянь:

- несанкціоноване втручання в роботу комп'ютерів;
- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;
- несанкціоновані збут або розповсюдження інформації з обмеженим доступом;
- несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах;
- порушення правил експлуатації та перешкоджання роботі комп'ютерів;

- шахрайства, вчинені з використанням електронно-обчислювальної техніки;
- порушення авторських прав шляхом незаконного відтворення комп'ютерних програм та баз даних;
- незаконні дії з банківськими платіжними системами;
- виготовлення, збут та розповсюдження порнографічних зображень цифрового формату.

Ефективність боротьби зі злочинами у сфері високих інформаційних технологій прямо залежить від використання комплексного підходу, потребує чіткого системного уявлення про їх сутність та масштаби, а також прогнозування майбутніх тенденцій і форм.

На початковому етапі розкриття та розслідування вказаних злочинів виникають труднощі у визначенні необхідної видової методики, оскільки часто ці види злочинів органічно доповнюють один одного, а суб'єкт їх вчинення може бути причетним до декількох різних злочинів цієї групи.

Для цього необхідно визначати пріоритетні напрями протидії, здійснювати програмно-цільове планування та належне ресурсне забезпечення, використовувати інноваційні методи попередження та розкриття.

Серед основних напрямків боротьби з організованою злочинністю слід окреслити:

- створення правової основи, організаційних, матеріально-технічних та інших умов для ефективної боротьби з організованою злочинністю, організація міжнародного співробітництва;
- виявляти та організовувати оперативне обслуговування інфраструктур, що обслуговують кримінальну діяльність у сфері високих інформаційних технологій;
- виявлення організованих злочинних угруповань, визначення напрямку спеціалізації, викриття їх міжнародних зв'язків;
- запобігання легалізації коштів, здобутих злочинним шляхом.

Специфіка злочинів у сфері високих інформаційних технологій зумовлює необхідність використання не тільки апаратних, але й програмних засобів пошуку фактичних даних. Аналіз оперативно-розшукової та слідчої діяльності переконливо свідчить про відсутність спеціального програмного забезпечення. Між тим вивчення відповідних інформаційних потоків дозволило б не тільки підвищити ефективність боротьби зі злочинами у сфері високих технологій, але й значно розширити можливості отримання оперативно значущої інформації за багатьма напрямками діяльності кримінальної міліції, надати нові можливості боротьби зі злочинністю в цілому [1, 86; 2, 89; 3, 36; 4, 35].

Єдність потенціалів та можливостей підрозділів органів внутрішніх справ істотно підвищує ефективність роботи. Як свідчать результати оперативно-слідчої практики, необхідною складовою розкриття та розслідування злочинів є постійне підвищення ефективності взаємодії. Очевидною є неспроможність держав індивідуально подолати високотехнологічну злочинність, якої притаманний міжнародний характер. За своїм змістом та ступенем суспільної небезпеки злочини у сфері високих інформаційних технологій впритул наблизились до міжнародних злочинів, оскільки спостерігається стійка тенденція використання глобалізаційних інформаційних процесів у кримінальних цілях. Вивчення правоохоронної діяльності зарубіжних країн, зокрема США, Великобританії, Німеччини, свідчить про масштабне застосування спеціально розроблених програмних комплексів для пошуку, фіксації і захисту необхідної інформації у цифровому форматі. Найбільш ефективними програмними комплексами виступають EnCase, Forensic Toolkit, та TSK [5, 35].

Для запобігання злочинам правоохоронні підрозділи США використовують комплекс заходів під умовною назвою “Fish bowling”, а німецькі правоохоронні підрозділи здійснюють аналогічну систему заходів “Honeynet”. В їх основі покладено імітацію активних потоків фінансової інформації банківських установ для виявлення та документування фактів незаконного підключення, а також географічного встановлення місцезнаходження правопорушників.

Для акумулювання позитивного зарубіжного досвіду правоохоронних підрозділів щодо протидії злочинності у сфері високих інформаційних технологій, організації міжнародного співробітництва та на цій основі розроблення відповідних методик розкриття та розслідування вказаних кримінальних діянь доцільно розглянути питання щодо створення наукової лабораторії на базі вищого навчального закладу системи МВС України. Це дозволить здійснювати постійне систематичне вивчення потреб практики як основи планування наукових досліджень, координацію наукових пошуків та своєчасно впроваджувати їх результати у практичну діяльність.

Література

1. Осипенко А.Л. Оперативно-розыскной мониторинг информационных ресурсов глобальных компьютерных сетей // Оперативник (сыщик). – 2009. – № 3(20). – С. 27–30.
2. Новицький А.М. Оперативно-розшукова діяльність в Інтернет: проблеми правозастосування // Правова інформатика. – 2009. – № 1(21). – С. 85–90.
3. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності // Право і Безпека. – 2009. – № 4 (31). – С. 214–220.

4. Бойченко О.В., Новиков М.М. Особливості оперативно-розшукової протидії комп'ютерній злочинності // Форум права. – 2010. – № 1. – С. 34–37.
5. Кэриэ Б. Криминалистический анализ файловых систем. – СПб.: Питер, 2007. – 480 с.

В.Г. Лісогор, *канд. юрид. наук, доц.,*
начальник відділу зв'язків з громадськістю та міжнародної діяльності
Національної академії внутрішніх справ

ОКРЕМІ ПРОБЛЕМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Кіберзлочинність є одним із видів злочинної діяльності, що розвиваються найбільш швидкими темпами. Це пов'язано з тим, що ця діяльність приносить надприбутки, які оцінюються фахівцями десятками мільярдів доларів. Серед факторів широкого розповсюдження кіберзлочинності є те, що на даний час комп'ютери та Інтернет стали невід'ємною частиною сучасного життя, а це дає змогу вчиняти злочини навіть не виходячи з дому, зокрема, можна вчинити незаконні дії на значній відстані від місця знаходження зловмисника, при цьому слідів такої діяльності практично не залишається. Фахівці наголошують на тому, що Інтернет являє собою глобальну систему. Це свідчить про те, що вчиненню злочинних дій за допомогою комп'ютерів і всесвітньої мережі у багатьох випадках не має можливості протиставити адекватні та своєчасні дії органів, що ведуть боротьбу з такими проявами, тим більше, що злочинець і жертва територіально можуть знаходитись на різних континентах, а це ускладнює відповідне реагування. Також звертається увага, що серед причин розповсюдження кіберзлочинності є те, що вчинення таких злочинів, як правило, не становить складності, відходять у минуле злочинці-одинаки, утворюються кіберугруповання, які працюють за принципами, подібними звичайним реальним компаніям, вони швидко розвиваються й стають організованими угруповання з розподілом функцій.

Злочини, що вчиняються з використанням комп'ютерів, і які можна віднести до кіберзлочинності, мають широкий спектр, до них належать різні фінансові махінації, комп'ютерні зламування, вірусні атаки, розповсюдження порнографії в Інтернет, крадіжки особистих даних, шпіонаж, шахрайство з кредитними картками та ін.

Слід підкреслити, що кіберзлочинність, окрім того, що вона приносить кримінальні надприбутки, вона завдає й значних збитків установам, організаціям, громадянам. Негативні наслідки такої діяльності також оцінюються великими сумами.

Необхідність боротьби з кіберзлочинністю вимагає відповідних дій з боку держав, їх урядів, розробки нормативних документів. У зв'язку

із цим виникають певні проблемні питання, пов'язані зокрема з тим, що окремі користувачі мережі Інтернет в Європі висловлюють стурбованість з приводу можливого порушення недоторканності їх приватного життя та свободи. Така стурбованість є реакцією на низку нормативних документів щодо боротьби з кіберзлочинністю, підготовлених відповідними інституціями Європейського Союзу.

Отже проблема, яка нині постала перед суспільством, має назву "кіберзлочинність", боротьба з нею є важливою і складною, вона вимагає великих зусиль та коштів, врахування всіх питань, пов'язаних із цим явищем, розробки стратегії і тактики її подолання, правового забезпечення. Протидія їй не обмежується національними кордонами, відповідні дії мають бути вчинені не окремою державою, а спільними узгодженими діями світового співтовариства із залученням відповідних інституцій. Розслідування, що розпочалося в одній країні, може продовжитися в іншій, а це свідчить про необхідність співпраці, оскільки без цього неможливо виявити злочинців і винести їм законний вирок.

І.М. Копотун, *канд. юрид. наук, заступник начальника*
Навчально-наукового інституту підготовки кадрів кримінальної міліції
Національної академії внутрішніх справ

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА НЕЗАКОННИХ ДІЙ З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ

Кримінальна відповідальність за підробку, використання та інші незаконні дії з банківськими пластиковими картками (БПК) передбачена ст. 200 КК України "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення". БПК є одним із предметів злочинного посягання, передбачених диспозицією цієї норми.

Банківська платіжна картка – спеціальний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу грошей з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування грошей зі своїх рахунків на рахунки інших осіб, отримання грошей у готівковій формі в касах банків і через банківські автомати (надалі банкомати), а також здійснення інших операцій, передбачених договором про карткове обслуговування (п. 1.27, ст. 1 Закону України "Про платіжні системи та переказ коштів в Україні").

Платіжні картки, що емітовані банками, поділяються на категорії залежно від статусу власника й держателя картки, рівня технічного обладнання, платіжної системи і платіжної організації. Вирізняють картки, випущені внутрідержавними (Національна система масових електронних платежів Національного банку України) і міжнародними ("VISA", "MASTER CARD", "AMERICAN EXPRESS" та ін.) платіжними системами. Залежно від схем розрахунків, вирізняють дебетові й кредитові картки.

Дебетовою є платіжна схема, що передбачає розрахунки за операції з платіжною карткою в межах власних коштів клієнта, які обліковуються на його картковому рахунку. Кредитною визнається платіжна схема, за якою здійснюються розрахунки та операції з платіжною карткою в межах кредиту, наданого банком клієнтові. Особливістю банківської кредитної картки є відкриття банком кредитної лінії, що використовується автоматично щоразу, коли купують товар або беруть кредит у грошовій формі.

Фізичним особам, які не є суб'єктами підприємницької діяльності, емітент надає особисті платіжні картки. Юридичні особи та фізичні особи-підприємці одержують корпоративні платіжні картки. Залежно від кредитної історії держателя картки, суми коштів на банківському рахунку, виділяють звичайні, срібні, золоті, та платинові картки. Залежно від типу носія ідентифікаційних даних, виділяють магнітні (картки з магнітною смугою) і так звані "смарткартки" (картки з електронним мікропроцесором), а також комбіновані, які містять і магнітну смугу, і електронний мікропроцесор (чіп). Картки, обладнані мікропроресорами, вважаються такими, що більш ефективно захищені від підроблень.

Загальні вимоги щодо порядку здійснення банками емісії платіжних карток, операції, що здійснюються з їх застосуванням, і порядок розрахунків за цими операціями визначає Положення "Про порядок емісії платіжних карток і здійснення операцій з їх застосуванням", затверджене Постановою Правління Національного банку України від 19 квітня 2005 р. № 137.

Порядок емісії та обігу банківських платіжних карток Національної системи масових електронних платежів встановлено Правилами Національної системи масових електронних платежів, затвердженими Постановою Правління Національного банку України від 10 грудня 2004 р. № 620.

Об'єктивна сторона злочину полягає у: підробці; придбанні; зберіганні; перевезенні; пересиланні; використанні; збуті підроблених БПК.

Підробкою є будь-які дії, унаслідок яких вносяться зміни до дійсної або створюється підроблена БПК, в результаті чого з її застосуванням можуть бути проведені незаконні (ініційовані не власником рахунка або не забезпечені наявністю грошей на банківському рахунку) перекази грошових коштів або ж доступ до інформації щодо певного банківського рахунка отримує не уповноважена на це особа. Придбання БПК полягає у оплатному або безоплатному придбанні її винною особою у інших осіб. Під зберіганням розуміють знаходження БПК безпосередньо у винного або в будь-якому іншому місці, де вони перебувають у розпорядженні та під контролем винного. Перевезенням БПК є її переміщення винним із використанням будь-яких транспортних засобів. Пересиланням слід вважати передачу чи спробу передачі БПК іншим особам з використанням поштового зв'язку, як Укрпошти, так і інших, міжнародних служб, які надають відповідні послуги ("UPS", "TNT", "DHL" та деякі інші). Передача БПК за допомогою водіїв міжміських автобусних маршрутів або провідників поїздів може також вважатися її пересиланням. Збутом БПК є її відчуження будь-яким способом: платним (шляхом продажу, обміну, використання у якості платежу) або безоплатним (дарування). При цьому особа усвідомлює, що збуває підроблений документ для його використання.

Під використанням підроблених БПК слід розуміти пред'явлення їх як справжніх з метою здійснення незаконного переказу грошових коштів, незаконного доступу до інформації щодо відповідного банківського рахунка тощо. Використанням підробленої платіжної картки слід вважати також спробу отримання з її допомогою грошових коштів через банківський автомат, здійснення з її застосуванням оплати товарів чи послуг, у тому числі в мережі Інтернет, коли надаються лише реквізити картки.

При вирішенні питання щодо кваліфікації дій за придбання, зберігання, перевезення, пересилання з метою збуту, використання чи збут, слід пам'ятати, що кримінальна відповідальність встановлена лише за такі дії з підробленими БПК. Злочин, залежно від способу, є закінченим з моменту вчинення однієї із дій, перелічених у ч. 1 ст. 200 КК.

Елементом об'єктивної сторони незаконних дій з БПК є спосіб вчинення злочину, зокрема: підроблення БПК; використання підроблених банківських платіжних карток; неправомірного внесення змін до інформаційних баз даних з використанням комп'ютерних технологій.

Суб'єктом злочину є будь-яка осудна особа віком від 16 років.

Суб'єктивна сторона злочину характеризується прямим умислом. Обов'язковою ознакою підробки, придбання, зберігання, перевезення, пересилання відповідних предметів закону є мета їх збуту.

Кваліфікуючими ознаками даного злочину є його вчинення:
1) повторно;
2) за попередньою змовою групою осіб.

При кваліфікації дій осіб за статтею 200 КК України слід враховувати особливості предмету, відрізняти цей злочин від інших складів злочинів, а також пам'ятати про недосконалості її чинного редакції. Незважаючи на наявність у назві статті такого предмету як "обладнання для їх виготовлення", у диспозиції він відсутній. Диспозиція цієї норми також не передбачає відповідальності за незаконне використання чужих БПК, хоча такі випадки трапляються у практиці доволі часто. Залежно від обставин ці дії можуть або взагалі не знайти своєї кримінально-правової оцінки або кваліфікуватися як готування чи замах до вчинення інших злочинів, зокрема, шахрайства.

З.І. Перощук, *доц. кафедри економіко-правових дисциплін*
Національної академії внутрішніх справ

ЗАПОБІГАННЯ ЗЛОЧИНАМ У СФЕРІ РОЗМІЩЕННЯ ТИМЧАСОВО ВІЛЬНИХ КОШТІВ МІСЦЕВИХ БЮДЖЕТІВ НА ВКЛАДНИХ (ДЕПОЗИТНИХ) РАХУНКАХ У БАНКАХ

Якщо вести мову про певну діяльність, яка полягає в усуненні причин та умов злочинності у сфері розміщення тимчасово вільних коштів місцевих бюджетів на вкладних (депозитних) рахунках у банках, відразу треба розуміти, що у даному випадку мова повинна йти про запобігання *злочинних дій, що здійснюються посадовими особами з використанням свого службового становища і завдають суттєвої шкоди* регіональним *суспільним інтересам* територіальних громад.

Кошти місцевих бюджетів – це бюджетні кошти, що передбачаються у місцевих бюджетах для забезпечення завдань і функцій, які здійснюються органами влади Автономної Республіки Крим та органами місцевого самоврядування протягом бюджетного періоду. За рахунок них надаються відповідні послуги громадянам кожної адміністративно-територіальної одиниці чи не в усіх соціально-культурних сферах, зокрема освіти, охорони здоров'я, соціального захисту та соціального забезпечення, культури і спорту. Кошти місцевих бюджетів відіграють значну роль у забезпеченні функціонування житлово-комунального господарства, засобів масової інформації, транспорту, дорожнього господарства тощо. Тому, будь-яке відволікання бюджетних коштів може призвести до неналежного виконання заходів, необхідних для нормального функціонування відповідних закладів, що надають перелічені вище послуги.

Слід звернути увагу, що розміщувати у банках, на вкладних (депозитних) рахунках, дозволяється тимчасово вільні кошти місцевих бюджетів, тобто той обсяг коштів, який не впливає на спроможність місцевого бюджету своєчасно і в повному обсязі здійснювати платежі за всіма його зобов'язаннями по кожній окремо взятій програмі.

Варто зауважити, що бюджетним законодавством забороняється витрачання бюджетних коштів на цілі, що не відповідають бюджетним призначенням, встановленим рішенням про місцевий бюджет, виділеним бюджетним асигнуванням чи кошторису, має наслідком зменшення асигнувань розпорядникам бюджетних коштів на суму коштів, що витрачені не за цільовим призначенням, і притягнення відповідних посадових осіб до юридичної відповідальності у порядку, визначеному законами України.

У свою чергу стаття 210 Кримінального кодексу України, використання службовою особою бюджетних коштів усупереч їх цільовому призначенню або в обсягах, що перевищують затверджені межі видатків, а так само недотримання вимог щодо пропорційного скорочення видатків бюджету чи пропорційного фінансування видатків бюджетів усіх рівнів, як це встановлено чинним бюджетним законодавством, інтерпретує як порушення законодавства про бюджетну систему України, за які передбачається певне покарання.

Виходячи із норм Бюджетного кодексу України визначитись із значенням терміну "тимчасово вільні кошти місцевих бюджетів" не можливо.

Постановою Кабінету Міністрів України це поняття трактується як обсяг коштів місцевого бюджету, які обліковуються на рахунках загального та/або спеціального фондів на дату їх розміщення на вкладних (депозитних) рахунках і відволікання яких не призведе до втрати платоспроможності місцевого бюджету та виникнення заборгованості за відповідним фондом місцевого бюджету протягом періоду, на який передбачається здійснити розміщення таких коштів на вкладних (депозитних) рахунках у банках.

Відповідно до статті 18 Закону України "Про Державний бюджет України на 2011 рік", Міністр фінансів Автономної Республіки Крим, керівник місцевого фінансового органу мають право за рішенням Верховної Ради Автономної Республіки Крим, відповідної місцевої ради в межах поточного бюджетного періоду здійснювати на конкурсних засадах розміщення тимчасово вільних коштів місцевих бюджетів на депозитах або шляхом придбання державних цінних паперів, цінних паперів, емітованих Автономною Республікою Крим, відповідною місцевою

радою, з подальшим поверненням таких коштів до кінця поточного бюджетного періоду.

У контексті вищевикладеного, потрібно чітко розуміти ту межу соціальної діяльності, яка полягає в усуненні причин та умов злочинності у сфері, про яку ведеться мова.

Якщо законодавством України дозволяється розміщення тимчасово вільних коштів місцевих бюджетів на депозитах, то тоді мають бути чітко визначені умови розміщення таких коштів на вкладних (депозитних) рахунках у банках, якими є:

- прийняття Верховною Радою Автономної Республіки Крим або місцевою радою відповідного рішення;
- визначення у договорі банківського вкладу (депозиту) між фінансовим органом та банком обов'язкових умов щодо права вкладника на повернення вкладу (депозиту) або його частини на першу вимогу вкладника та щодо заборони безспірного списання банком коштів з вкладного (депозитного) рахунка фінансового органу, а також відповідальності банку у разі неповернення чи несвоєчасного повернення коштів з вкладних (депозитних) рахунків на відповідні рахунки місцевих бюджетів, відкриті в органах Державного казначейства, з яких перераховувалися тимчасово вільні кошти для розміщення на вкладних (депозитних) рахунках;
- відсутність на дату розміщення тимчасово вільних коштів простроченої кредиторської заборгованості за відповідним фондом місцевого бюджету (відповідними напрямами його використання), крім тієї, що виникла внаслідок недоотримання коштів субвенцій з державного бюджету та бюджетів інших рівнів;
- розміщення на конкурсних засадах тимчасово вільних коштів виключно в державних банках та банках, у капіталізації яких взяла участь держава.

Варто зазначити, що порушене питання є надзвичайно актуальним, так як мова йде про фінансові ресурси, необхідні для забезпечення функцій та повноважень місцевого самоврядування. А відволікати бюджетні кошти, як зазначалося вище, можна лише у тих випадках, коли місцевий бюджет спроможний своєчасно і в повному обсязі здійснювати платежі за всіма його зобов'язаннями по кожній окремо взятій програмі.

Так, до основних форм запобігання злочинам у сфері розміщення тимчасово вільних коштів місцевих бюджетів на вкладних (депозитних) рахунках у банках належать:

- проведення комплексних перевірок законності розміщення тимчасово вільних коштів місцевих бюджетів на вкладних (депозитних) рахунках у банках;
- перевірка правильності здійснення процедури розміщення таких коштів;
- своєчасне запобігання, розкриття та розслідування виявлених у цій сфері злочинів;
- висвітлення у засобах масової інформації стану злочинності у сфері розміщення тимчасово вільних коштів місцевих бюджетів на вкладних (депозитних) рахунках у банках і напрямів боротьби з нею;
- створення відповідного механізму фінансового контролю, який би був заснований на організаційній взаємодії бюджетних та банківських органів;
- відшкодування нанесених територіальній громаді збитків.

Варто відзначити, що на сьогодні мабуть досить складно спрогнозувати можливість попередження протиправних дій у сфері розміщення тимчасово вільних коштів місцевих бюджетів на вкладних (депозитних) рахунках у банках. Пояснюється така позиція тим, що у переважній більшості відсутній необхідний рівень кваліфікації працівників відповідних підрозділів, в першу чергу, органів внутрішніх справ.

На нашу думку, у цьому напрямі доцільно було б:

- здійснювати цілеспрямований відбір до відповідних підрозділів органів внутрішніх справ фахівців фінансово-бюджетних галузей, на яких буде покладений обов'язок здійснювати оперативне обслуговування та розслідування кримінальних справ цієї категорії;
- на базі навчальних закладів МВС організувати спільні для працівників відповідних підрозділів органів внутрішніх справ курси підвищення кваліфікації, які виявляють та розслідують злочини, пов'язані з порушенням законодавства про бюджетну систему України, в тому числі у частині розміщення тимчасово вільних коштів місцевих бюджетів на вкладних (депозитних) рахунках у банках;
- регулярно організувати проведення занять, з метою доведення та аналізу нових змін у законодавстві, оскільки практичні працівники органів внутрішніх справ у зв'язку з великою завантаженістю реально не встигають прослідкувати та аналізувати нові зміни і в законах, і в підзаконних нормативно-правових актах, що регулюють відносини у сфері бюджетної системи України.

І.В. Рогатюк, *канд. юрид. наук, ст. науковий співробітник,*
заслужений юрист України, ст. помічник Генерального прокурора;
О.В. Калиновський, *канд. юрид. наук,*

заступник начальника відділу організації науково-дослідної роботи
Національної академії внутрішніх справ

ПІДСТАВИ І ПОРЯДОК ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНОЇ СПРАВИ

Відповідно до ч. 1 ст. 28 Закону України "Про інформацію" режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом, у свою чергу, поділяється на конфіденційну і таємну (ч. 1 ст. 30 Закону).

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної.

Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України. До конфіденційної інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, не можуть бути віднесені відомості: про стан довкілля, якість харчових продуктів і предметів побуту; про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян; про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення; стосовно стану справ із правами і свободами людини і громадянина, а також фактів їх порушень; про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб; інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути обмеженим.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та

іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

Водночас у деяких чинних нормативних актах в поняття "конфіденційність" вкладено інший зміст. Так, у п. 13 ст. 8, ч. 2 ст. 11 Закону України "Про оперативно-розшукову діяльність", п. 9 ст. 25, ч. 4 ст. 28 Закону України "Про Службу безпеки України", п. 4 ст. 6 Закону України "Про державну таємницю" вказано про конфіденційне співробітництво і конфіденційність відносин з громадянами, які сприяють діяльності оперативно-розшукових підрозділів. Враховуючи специфіку їх роботи, вочевидь тут мається на увазі не обмеженість доступу до інформації з боку інших осіб, а неприпустимість розголошення про таке співробітництво, його таємність. Саме цю обставину фактично підтверджують положення частини третьої статті 11 Закону України "Про оперативно-розшукову діяльність". Про те, що відомості конфіденційного характеру, отримані посадовими особами по підтриманню правопорядку, зберігаються у таємниці, якщо виконання обов'язків або вимоги правосуддя не вимагають іншого, вказується також у статті 4 Кодексу поведінки посадових осіб по підтриманню правопорядку, затвердженого резолюцією № 34/168 Генеральної Асамблеї ООН 17 грудня 1979 р.

До таємної належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію. Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених Законом України "Про інформацію". Порядок і терміни оприлюднення таємної інформації визначаються Законом України "Про державну таємницю".

Комерційна таємниця – сукупність відомостей технічного, організаційного, комерційного, виробничого та іншого характеру становить значний економічний інтерес для її власника, що провадить господарську діяльність в умовах конкуренції. Забезпечення належного правового регулювання відносин, пов'язаних з охороною комерційної таємниці,

є важливим завданням в рамках реалізації державної політики у сфері розвитку економічної конкуренції та обмеження монополізму.

За неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею, винні особи несуть відповідальність, встановлену законом. На сьогодні законодавство з питань комерційної таємниці не систематизовано. Відносини, пов'язані з охороною комерційної таємниці, регулюються нормативно-правовими актами, що належать до різних галузей права, зокрема Цивільним кодексом України, Господарським кодексом України, Кримінальним кодексом України, Кодексом України про адміністративні правопорушення, Законами України "Про інформацію", "Про науково-технічну інформацію", "Про захист від недобросовісної конкуренції", і визначають лише загальні засади правового регулювання таких відносин.

Банківська таємниця – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту (ст. 60 Закону України "Про банки і банківську діяльність").

Банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;
3) фінансово-економічний стан клієнтів;
4) системи охорони банку та клієнтів;
5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;
6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;
8) коди, що використовуються банками для захисту інформації.

Національний банк України видає нормативно-правові акти з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів.

Банки зобов'язані забезпечити збереження банківської таємниці шляхом:

1) обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю;

2) організації спеціального діловодства з документами, що містять банківську таємницю;
3) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
4) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками:
1) на письмовий запит або з письмового дозволу власника такої інформації;
2) на письмову вимогу суду або за рішенням суду;
3) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;
4) органам Державної податкової служби України на їх письмову вимогу з питань оподаткування або валютного контролю стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;
5) спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу на його письмову вимогу стосовно додаткової інформації про фінансову операцію, що стала об'єктом фінансового моніторингу;
6) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів стосовно стану рахунків конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності.

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:
1) бути викладена на бланку державного органу встановленої форми;
2) бути надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою;
3) містити передбачені цим Законом підстави для отримання цієї інформації;
4) містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Обмеження стосовно отримання інформації, що містить банківську таємницю, передбачені цією статтею, не поширюються на службовців Національного банку України або уповноважених ними осіб, які в межах повноважень, наданих Законом України "Про Національний банк

України", здійснюють функції банківського нагляду або валютного контролю.

І.В. Європіна, *завідуючий кафедрою*
Національної академії прокуратури України

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТРАНСНАЦІОНАЛЬНОЇ КОМПЮТЕРНОЇ ЗЛОЧИННОСТІ В СУЧАСНОМУ СВІТІ

Стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет та спрощення доступу до неї широкого кола користувачів через персональні комп'ютери – обумовили зростання злочинних проявів транснаціонального (трансграничного) характеру. Достатньо проаналізувати нижченаведені цифри, щоб зрозуміти, яку загрозу для національної безпеки держави, її економічної та інформаційної складових представляє розширення масштабів користування названою інформаційною мережею, при вкрай недостатньому контролі за проходженням інформації з боку держави.

Послуги доступу до глобальної мережі Інтернет в Україні надають більше 1 600 підприємств, зокрема, 624 Інтернет-провайдера та більше 1 000 Інтернет-клубів (Інтернет-кафе). Також, в українському сегменті мережі Інтернет створено 873 Інтернет-портали та 1 912 Інтернет-магазинів. Кількість користувачів мережі Інтернет в Україні становить близько 4 млн. осіб. Стаціонарним телефонним зв'язком в Україні користуються більше 12,5 млн. абонентів, з яких близько 10 млн. абонентів обслуговує ВАТ "Укртелеком". Майже 1 млн. абонентів обслуговують приватні оператори зв'язку. Мережею мобільного зв'язку в Україні користуються близько 49 млн. абонентів.

В Україні набули поширення наступні служби переказів: служби поштових переказів Western Union – 17 банків-агентів, Money Gram – 11 банків-агентів, система банківських переказів Anelik – 52 банки-агенти.

Швидкими темпами розвиваються позабанківські електронні платіжні системи. Так, серед позабанківських систем розрахунків on-line (в режимі реального часу) самою поширеною є WebMoney. До її системи на даний час належать: пункти поповнення WM гаманців – 586, обмінних пунктів – 43, реєстраторів – 9, персоналізаторів – 25, WM дилерів – 32, точок продажу WM карт – 260, пунктів поповнення WM гаманців готівкою – 251.

Аналіз статистичних даних і криміногенної ситуації свідчить, що найбільш поширеними видами злочинів в Україні у сфері інформаційно-телекомунікаційних технологій є [1]:

- несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж; – несанкціонований збут та розповсюдження інформації з обмеженим доступом;
- шахрайство з використанням комп'ютерної техніки, шахрайство в мережі Інтернет;
- шахрайство з боку операторів зв'язку та абонентів телекомунікаційних компаній;
- підробка банківських платіжних карток.

Крім цього, в Україні поширені наступні види комп'ютерних зловживань:

- виготовлення та розповсюдження шкідливих комп'ютерних програм;
- порушення правил експлуатації комп'ютерних та телекомунікаційних мереж;
- несанкціонована зміна маршрутизації міжнародного телефонного трафіку.

Самостійним видом злочинної діяльності стало викрадення ідентифікаційних даних осіб, з метою отримання доступу до банківських рахунків, безоплатного користування послугами Інтернет-провайдерів та операторів зв'язку [2, 35].

У структурі злочинних діянь, викритих у сфері інформаційно-телекомунікаційних технологій, 26 % складають злочини у сфері комп'ютерних та Інтернет-технологій, 28 % – у сфері функціонування електронних платежів або платіжних карток, 16 % – у сфері телекомунікацій. Решта – пов'язана з використанням комп'ютерних технологій при вчиненні традиційних злочинів.

Трансграничне "нелегальне інформаційне брокерство" як різновид організованої комп'ютерної злочинності з'явився нині в багатьох країнах світу, де отримав назву "нелегальне інформаційне брокерство". Особи, які цим займаються, за допомогою спеціально створених комп'ютерних програм долають системи технічного захисту інформації в автоматизованих (комп'ютерних) системах – комп'ютерних мережах, отримують з автоматизованих баз даних інформацію, а потім її продають. Покупцями виступають як конкуруючі організації (фірми), так й інші юридичні та фізичні особи.

Організоване промислове (комерційне, підприємницьке) шпигунство представляє собою придбання протиправними засобами або відкриття, переміщення чи використання торгової, комерційної, промислової таємниці без відповідного дозволу або інших законних підстав з ме-

тою заподіяння економічної шкоди особою, яка допущена до таємниці, або одержання протизаконної економічної переваги для себе або інших осіб. За висновками експертів, збитки від розвідувальної діяльності конкурентів, що використовують методи шпигунства, складають до 30 % всіх світових збитків, а це – мільярди доларів США. Масштаби цього виду злочинної діяльності можна оцінити хоча б за таким прикладом: на виставці-продажу апаратури технічної розвідки та контррозвідки у 1995 році було продано 70 тис. одиниць апаратури добування інформації і лише одиниці їх пошуку і знешкодження. А всього було виставлено більше ніж 2 000 видів приладів технічного добування і захисту інформації.

Організоване "комп'ютерне піратство". Дослідження цієї проблематики, проведені у 70 країнах світу на замовлення Асоціації виробників комп'ютерних програм (B8A) і Асоціації видавців комп'ютерних програм (8PA) засвідчили, що із 523 млн. нових прикладних комп'ютерних програм ділового призначення майже кожна друга (225 млн. одиниць) є неліцензійною копією. Збитки світових виробників внаслідок "піратської індустрії" комп'ютерного програмного забезпечення сягають десятки мільярдів у.о. на рік. Найвищий показник збитків від "комп'ютерного піратства" належить Південній Америці [3, 12]. За високим рівнем "комп'ютерного піратства" визначаються також: В'єтнам – 99 %; Китай – 96 %; Оман – 95 %; Німеччина – 36 %, Данія – 35 %; Нова Зеландія – 35 %; Великобританія – 34 %; США – 27 % [4, 39]. У країнах Східної Європи в числі лідерів "комп'ютерного піратства" Словенія – 96 %; Болгарія – 94 %; Румунія – 93 %; Росія – 90 %; Україна – 90 %; Чехія – 62 %; Словаччина – 62 %. Річний обсяг збитків розробників комп'ютерних програм у грошовому обчисленні перевищує 700 млн. у.о. [5, 52].

Не меншої шкоди завдають світовому співтовариству і крадіжки, що вчиняються за допомогою транснаціональної мережі Інтернет. Щорічно це близько 5 мільярдів у доларовому еквіваленті. Лише протягом одного року, канадська митна служба, використовуючи спеціальне обладнання, змогла викрити та попередити 800 таких фактів, вчинених за допомогою незаконних операцій з електронними пластиковим картками [6, 23].

Одним з найпоширеніших видів транснаціонального характеру є шахрайства в Інтернет-торгівлі. Від злочинів цього виду зазнають шкоди електронна комерція, торгівля цінними паперами, купівля-продаж товарів у *віртуальних магазинах*, посередницькі операції та управління майном.

Більше за все шахрайства такого роду поширені в країнах з розвинутою економікою, де існує розгалужена мережа Інтернет-торгівлі

(Японія, США, Канада, Південна Корея, Австралія, держави-члени Європейського Союзу тощо), і де вживається заходів до удосконалення всіх інших напрямів комерційної діяльності, приміром, через надання преференцій у вигляді звільнення від оподаткування. У США, наприклад, до якомога активнішого використання можливостей Інтернет-торгівлі закликає бізнесменів сам Президент країни, за що обіцяє їм податкові та інші пільги.

Дослідження, що проводилось одним з університетів у штаті Техас (США), встановило, що торік американські компанії одержали від "он-лайнового" продажу товарів і послуг понад $301 млрд. Цей розмір встановлений аналітиками на основі опитування приблизно 3 000 компаній, що використовують Інтернет у своїй діяльності. Обсяг продажу через таких посередників, як біржові маклери й турагенства, склав $58 млрд. Вражає також розмір інвестицій американських компаній у Інтернет: на програмне забезпечення, консалтингові послуги, навчання, обслуговування тощо ними витрачено $56 млрд., а на комп'ютери і програмне забезпечення для самих нижніх рівнів глобальної комп'ютерної мережі – ще $115 млрд. Якщо брати до порівняльної характеристики ці кошти, вони співставимі лише з оборотами в таких головних секторах американської економіки, як автомобілебудування та зв'язок.

Крім незаконного одержання послуг, сучасні засоби телекомунікацій і глобальна комп'ютерна мережа Інтернет відкривають перед злочинцями нові можливості в таких сферах шахрайської діяльності, як, наприклад, незаконна організація азартних ігор (електронне казино, незаконна *лотерея*, тоталізатори: спортивний, політичний тощо). Цілком нові можливості, засновані на властивостях електронної пошти, груп електронних новин і сервісу, що забезпечуються Всесвітнім павутинням – WWW (World Wide Web), відчиняються перед шахраями в галузі організації фінансових пірамід, фіктивних *шлюбних контор*, *бюро працевлаштування*, фірм по наданню *міфічних послуг*, продажу "повітря" тощо. В усіх цих випадках нові засоби забезпечують величезну швидкість взаємодії з потенційними жертвами й анонімність самого шахрая. Інші напрямки шахрайства засновані на модифікації інформації, що відображає електронні безготівкові фінанси. Існує декілька вже достатньо відомих шахрайств такого роду. Наприклад, несанкціонований доступ до електронних банківських рахунків і модифікація інформації, що знаходиться в них. Для того, щоб не порушувався загальний баланс банківських операцій, електронні кошти переписуються на рахунках клієнтів банку і на рахунках, доступних злочинцям. Таким чином, на рахунки, контрольовані злочинцями, "перетікають" фінанси клієнтів, які нічого не підозрюють.

За твердженням засновника сервісу E-Serute-IT Арджена де Ландграфа, найбільшу небезпеку представляють "російські рибаки", які не тільки займаються виуджуванням інформації у клієнтів банків, але й загрожують атаками на сайти кредитних установ, що намагаються їм протидіяти. Він наводить приклад одного австралійського банку, нормальне функціонування якого було порушено протягом трьох днів що спричинило колосальні матеріальні збитки. Доходи від цього виду злочинної діяльності становлять в середньому $150 млн. на рік [7, 16].

Класичним прикладом банківського шахрайства вважається "справа Левіна", що віднесена міжнародною кримінальною поліцією до категорії "транснаціональних мережевих комп'ютерних злочинів". Дотепер залишається відкритим питання, як В. Левіну і його поплічникам вдалося одержати доступ до подвійних паролів й ідентифікаторів клієнтів, що використовуються у системі керування грошовими операціями (векселедавець/контролер). Є припущення, що злочинці мали спільників серед персоналу "Сіті-банку". Фахівці з захисту інформації вважають, що одержанню паролів сприяла особливість серверу системи керування грошовими операціями, при підключенні до якого через систему передачі даних "Спринт/Теленет" відразу після короткочасного перериванння чергового сеансу новий абонент сприймався, як попередній клієнт, з усіма доступними йому привілеями. Саме через це, злочинцям вдавалося видавати себе за власників рахунків.

Шахрайські операції проводилися в правильному форматі даних, зі справжніми номерами, ідентифікаторами й паролями клієнтів. Злочинний намір шахраїв передбачав здійснення порядку 40 переказів, на суму близько 10 млн. доларів, проте, реально їм вдалося здійснити менше половини із них, на суму 400 тис. доларів. Рахунки постраждалих знаходилися в США, Канаді, Мексиці, Аргентині, Новій Зеландії, Колумбії, Гонконзі, Індонезії та Уругваї. Перекази відправлялися до США, Росії, Фінляндії, Нідерландів, Німеччини, Швейцарії та Ізраїлю.

Завдяки оперативності й злагодженості дій працівників служби безпеки банку та співробітників ФБР була проведена широкомасштабна поліцейська операція на території 14 країн, що дозволило вийти на офіс фірми АТ "Сатурн" у Санкт-Петербурзі, а відтак і на членів злочинного угруповання, до складу якого входили громадяни Росії В. Левін, О. Шустер, Є. і К. Королькови, А. Ламін, Д. Чадаев, О. Лачманов (він же А. Палимідес), В. Воронін (він же А. Лисенков), М. Графінін, Ю. Тарка, а також громадяни Нідерландів Франс Бул і Рік Ван Везель.

Одним із способів банківського шахрайства є модифікація алгоритмів, що визначають функціонування системи опрацювання інформації

про безготівкові банківські розрахунки. Відомі випадки зміни коефіцієнта перерахунку курсу валют. При цьому клієнтам банку валюта перераховується по заниженому курсу, а різниця заноситься на рахунки, що контролюються злочинцями. Більш витончений спосіб, заснований на округленні до цілого нарахованих клієнту відсотків при виплаті. Результат округлення, природно, зараховується на рахунок злочинця. Подібні операції через малі суми, що викрадаються, практично залишаються непоміченими і для клієнтів, і для керівництва банку. Проте, у зв'язку з тим, що одночасно опрацьовується велика кількість рахунків, викрадені кошти можуть складати значні суми. У спеціальній літературі протиправне діяння, вчинене у такий спосіб, називається "салямі", тому що викрадені кошти надходять малими порціями – шматочками.

Характерним прикладом злочинів цього виду може бути шахрайство у Зовнішекономбанку (ЗЕБ), вчинене громадянином Б. за попереднім зговором із персоналом цього банку. Зауважимо, що притягти до кримінальної відповідальності службовців ЗЕБ правоохоронним органам не вдалося по причині відсутності прямих доказів їх провини.

Технологія шахрайства включала декілька етапів. На першому із них, на окремих, повторно відкритих валютних рахунках, шляхом коригування записів в архіві банківської інформації, були створені надлишки валютних засобів у сумі приблизно 1,5 тис. доларів із зміною власників. На другому етапі, при переході ЗЕБ до комерційного валютного курсу, незаконні суми були збільшені втроє. На третьому етапі, при перерахунку карбованцевих залишків на рахунках, відкритих у фінських марках (у зв'язку зі скасуванням клірингової системи розрахунків із Фінляндією), була проведена операція типу "салямі", тобто додатково були організовані приписки у файлах банківської інформації. Таким чином, без оформлення відповідних проводок на фіктивні рахунки з кодом фінських марок, були тимчасово переведені кошти з рахунків з іншими кодами валют. Потім, після перерахунку, запозичені суми були повернуті зворотно. В результаті цієї операції курсова різниця склала більш 1,9 млн. інвалютних карбованців. Наслідком злочинної діяльності стало виведення біля 1 млн. доларів з-під автоматизованого врахування, із них 125 тис. громадянину Б. вдалося отримати за підробленими паспортами. Суд засудив громадянина Б. до тривалого терміну позбавлення волі.

Література

1. Как ограбить Интернет: Украина поможет / [М. Крамаренко]. – Джерело: http:/ sngnews.ru / 11 жовтня 2007 р.

2. Аналітичний огляд протидії комп'ютерної злочинності в Україні у 2003 році – за результатами діяльності підрозділів ДСБЕЗ / [За ред. В.В. Шапоренко.]. – К.: Департамент ДСБЕЗ МВС України. – 2004.
3. Организация и современные методи защиты информации / [под общ. ред. С. Диева, А. Шаваева]. – М.: "Банковский деловой центр". – 1998.
4. Галицькі контракти. – 1998. – № 11, с. 39.
5. Зарубіжний досвід попередження шахрайств з використанням пластикових карток: збірник наукових праць / [О. Юрченко]. – Інформаційні технології та захист інформації. – 1998. – № 2.
6. Computer World. – К., – 2000. – № 13(272).
7. Електронний банкінг у контексті захисту персональних даних: наукове видання / [За ред. В. Брижко, Ю. Базанова, М. Швець]. – Київ, 2008.

О.О. Волков, *ст. слідчий в особливо важливих справах*
Головного слідчого управління МВС України

ЗЛОЧИНИ В БАНКІВСЬКІЙ СФЕРІ, ЩО ВЧИНЯЮТЬСЯ ЗА ДОПОМОГОЮ СПЕЦІАЛЬНО СТВОРЕНИХ ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ

Яскраво виражена соціальна нерівність в Україні між бідними людьми, людьми з середнім достатком та багатими являє собою яскравий приклад третіх країн або країни що розвиваються. В цій ситуації добробут одних провокує інших з меншим достатком займатися протиправними видами діяльності, а саме написанням шкідливих програмних засобів, які дозволять викрадати банківські реквізити клієнтів. Такі шкідливі програмні засоби спеціально створюються для банківських установ і призначені для викрадення інформацію про банківських клієнтів називаються банкерами.

Враховуючи те, що в Україні розвинута система інтернет-банкінкгу, такий вид злочинної діяльності багатьом може здатися досить прибутковим. В Україні, за даними Національного Банку України, загальна кількість емітованих банками платіжних карток складає 44,201 млн. штук. Сума операцій з використанням платіжних карток, емітованих українськими банками, склала 92,850 млрд. грн., з яких більше 93 %, – отримання готівки. Кількість банкоматів в Україні за 1-й квартал 2010 року склала 28 305 одиниць. Як повідомляє НБУ 146 українських банківських установ є членами міжнародних карткових платіжних систем, що значно збільшує кількість користувачів і кількість таких транзакцій [1].

З розвитком банківської інфраструктури, розширення переліку послуг, що надаються банківськими установами збільшується кількість злочинів пов'язаних з несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем,

комп'ютерних мереж. З огляду на викладене слід виділи наступні тенденції розвитку кіберзлочинності в банківській сфері в Україні:

1. Темпи росту банківського технічного устаткування.
2. Корисна мотивація більшості вчинених комп'ютерних злочинів.
3. Ускладнення способів вчинення комп'ютерних злочинів і поява нових видів протиправної діяльності в сфері комп'ютерної інформації.
4. Ріст кримінального професіоналізму комп'ютерних зловмисників.
5. Омолодження віку комп'ютерних зловмисників і збільшення кількості осіб, що раніше не притягувалися до кримінальної відповідальності.
6. Ріст матеріального збитку від комп'ютерних злочинів в загальній кількості збитків від інших видів злочинів.
7. Перенесення уваги на вчинення злочинної діяльності з використанням комп'ютерних мереж.
8. Перехід комп'ютерної злочинності в розряд транснаціональної.
9. Високий рівень латентності кіберзлочинності в банківській сфері.

Саме, кількість клієнтів та механізм захисту який використовує та чи інша банківська установа в певній мірі є переважаючим фактором у виборі об'єкта посягання. Технологічність вчинених злочинів в банківській сфері в першу чергу залежить від захищеності комп'ютерних мереж тоєї чи іншої банківської установи. В залежності від технологічності механізму вчинення злочину залежать і збитки від нього. В запропонованій схемі злочинної діяльності в банківській сфері на останньому місці вказано найбільш технологічні та такі, що приносять найбільший збиток для банківських установ.

1. Всілякі види викрадення готівки з банківських установ (крадіжки, грабежі, розбої, шахрайства).
2. Такі ж види злочинів тільки заволодіння банківськими картками.
3. Щупи, накладки, що блокують картку в банкоматі та подальше їх використання правопорушниками (примітивні пристрої).
4. Скимери, накладки, мініатюрні відеокамери, що дозволяють перехоплювати інформацію користувача банкомата (електронні пристрої 1-го покоління).
5. Шимери, перехоплюючи пристрої з високим рівнем мінімізації розмірів, їх висока маскувальність та більш розширені функції перехоплення інформації з банківської картки (електронні пристрої 2-го покоління).
6. Електронні пристрої які дозволяють перехоплювати інформацію з банківської картки користувача та обміну інформацією банкомату з центральним сервером за допомогою електромагнітного та інших ви-

дів випромінювання – без механічного втручання в роботу банкомату (електронні пристрої 3-го покоління).

7. Банкери – шкідливі програмні засоби спеціально призначені для викрадення банківської інформації як в клієнтів банку так і в самих банківських установах.

У своєму виступі ми хочемо звернути увагу на найбільш технологічний вид злочинної діяльності, який спричиняє найбільші на цей час збитки для банківських установ. Такий вид протиправної діяльності пов'язаний з несанкціонованим втручанням в операційну систему банківського серверу, банкомату, комп'ютерну мережу банкомату для крадіжки грошей і отримання інформації про рахунки клієнтів банківської установи. Для цього спеціально створюються та розповсюджуються шкідливі програмні засоби, які самостійно або цілеспрямовано поширюються зловмисником комп'ютерними мережами та мережами електрозв'язку.

Слід зазначити, що банкери, як особливість таких шкідливих програмних засобів, не поширюються як окремі файли. В процесі ураження комп'ютера користувача завжди встановлюється цілий комплекс додаткових шкідливих програмних модулів.

Характерні особливості банкерів:

1. Невеликий об'єм програмного засобу.
2. Певна автономність кожного модуля.
3. Вузька спеціалізація такого програмного засобу.

Зловмисники проводять комплексну атаку і збирають будь-які іншу інформацію що може бути їм корисною, а не зосереджують свою увагу лише на банківській інформації. Класична схема ураження шкідливими програмними засобами комп'ютерів клієнтів різних банків відбувається за однотипним сценарієм.

З самого початку на сервері знаходиться троянська програма, яка не розпізнається антивірусними засобами та іншими засобами захисту комп'ютера як шкідлива і повинна завантажити та інсталювати в систему всі інші шкідливі програмні модулі:

1. Програму, що краде інформацію користувачів соціальних мереж.
2. Програму, що бореться з антивірусними системами.
3. Один чи два банкери, які повинні моніторити всі з'єднання з банком, перехоплювати їх і передавати пароль та ім'я користувача зловмиснику.

Основне місце, через яке поширюються шкідливі програмні засоби це веб-сторінки інтернеті. У випадках коли злочинцями сплановано серйозну справу ними створюється довго живучий Інтернет-ресурс,

з використанням техніки визначення IP-адреси потенційної жертви. Знання IP-адреси користувача що завантажив (перегладає) уражену веб-сторінку, дозволяє зловмиснику вести направлені атаки і приховувати шкідливі програмні засоби від антивірусних програм.

Для того щоб клієнт зайшов на сторінку з розміщеним шкідливим програмним засобом їх туди заманюють за допомогою: спамових листів, які нібито містять повідомлення самого банку (у тексті листа якого розміщена зноска нібито на сайт банку. Користувач саме з тексту листа може зайти на сторінку банку. Але це сторінка не банку, а зроблена під його сторінку сайт зловмисників) або новини пов'язані з життям країни, політичних діячів або поп-зірок. Також розсилається так званий порно-спам. В будь-якому випадку посилання в тексті листа спаму веде користувача на уражений ресурс.

Той факт, що зловмисники зламують веб-сторінки банків, свідчить про те, що вони працюють організованою групою. Кожен член групи має свою спеціалізацію: написання шкідливого коду, хакінг, прикриття своєї діяльності та видалення слідів перебування у мережі, переведення в готівку викрадених грошей та подальша їх легалізація і т.п. Таким чином, за конкретним злочином проти банківської установи як правило стоять не одинаки, а групи кіберзлочинців, в які входять молоді люди з малозабезпечених сімей. Жага швидкої наживи визначає зміст їх життя: створення шкідливого програмного засобу, їх розповсюдження серед користувачів, викрадення за їх допомогою грошей, їх витрачати і знову займатися тим же самим. З такого замкнутого порочного кола, молодим людям вирватися дуже складно.

Якщо мова йде про великі суми грошей, використовують посередників, через рахунки яких проходить перша транзакція з рахунку жертви. Посередники, у свою чергу, пересилають гроші на третій рахунок, отримуючи за це певний відсоток. Коли ж мова йде про дрібні суми, вкрадені з рахунків (200–500 доларів), то в основному гроші переводяться безпосередньо на рахунки зловмисників прямими транзакціями.

Підсумовуючи викладене слід зазначити, що одним з факторів успіху злочинців є досить низький рівень підготовки в області інтернет-безпеки користувачів інтернету – клієнтів банку. З іншого боку банківськими установами вживаються лише мінімальні заходи що забезпечують безпеку своїх клієнтів.

На сьогоднішній день банківські установи намагаються уникати публічних розслідувань та інцидентів що не поліпшує ситуацію та не призводить до дієвих результатів боротьби з кіберзлочинністю. В цьому плані очевидним є також і те, що необхідно працювати над новими схемами обміну інформацією між банківськими установами та пра-

воохоронними органами країни для протидії кіберзлочинності в банківській сфері.

Література

1. http://www.bank.gov.ua/.

Д.О. Алексєєва-Процюк, *канд. іст. наук, науковий співробітник наукової лабораторії проблем запобігання та розкриття тяжких злочинів;*
О.В. Процюк, *канд. юрид. наук, заступник начальника кафедри кримінального права, Національна академія внутрішніх справ*

КІБЕРЗЛОЧИНИ ВІДПОВІДНО ДО КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

В останній час все збільшується загроза, пов'язана з криміналізацією інформаційної сфери взагалі і Інтернету зокрема. Відкритість Інтернету породжує його високу уразливість від суспільно небезпечних і у тому числі злочинних посягань. Відомо, що пропорційно розширенню Мережі росте число кіберзлочинів. Спам, дитяча порнографія і електронні розкрадання та інші злочини стали невід'ємною рисою сучасних інформаційних процесів. Злочинці, за допомогою міжнародних комп'ютерних мереж розповсюджують свій кримінальний досвід, а також вчиняють злочини, не звертаючи увагу на національні кордони, що вимагає відповідних кроків кооперації від поліцейських установ різних країн. Ефективна боротьба із кіберзлочинністю вимагає більш дієвого та ефективно функціонуючого співробітництва правоохоронних органів різних країн.

Органами внутрішніх справ України, при розкритті трансграничних злочинів, для взаємообміну інформацією з правоохоронними органами інших країн активно використовуються канали Інтерполу, а також можливості Управління міжнародних зв'язків МВС України, апаратів представників правоохоронних органів (як представників МВС України за кордоном, так і представників правоохоронних органів інших країн в Україні).

На даний час в Україні працюють представники МВС Австрійської Республіки, Королівства Бельгії, Республіки Білорусь, Федеративної Республіки Німеччини, Республіки Польща, Французької Республіки, Чеської Республіки, Королівства Данії. Відповідальний за Україну представник поліції Держави Ізраїль знаходиться у Москві (Російська Федерація), представник поліції та митниці Королівства Швеції – у Будапешті (Угорщина). Представники МВС України за кордонам знаходяться в Республіці Польща, Федеративній Республіці Німеччини, Державі Ізраїль.

На даний час є досить багато нормативних актів, що регулюють діяльність в сфері міжнародного співробітництва з правоохоронними органами інших країн щодо протидії злочинності у сфері високих технологій. Одним із них є Конвенція про кіберзлочинність від 07.09.2005. В сучасній науковій літературі ведуться дискусії щодо визначення поняття кіберзлочинів. Даною Конвенцією кіберзлочинами пропонується визнавати цілий ряд правопорушень:

- **Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, що включає: незаконний доступ** – навмисний доступ до цілої комп'ютерної системи або її частини без права на це, вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою (кваліфікується за ст. 361, ст. 361-2, 363-1 КК України); **нелегальне перехоплення** – навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані, вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою (кваліфікується за ст. 361 КК України); **втручання у дані** – навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це (кваліфікується за ст. 361 КК України); **втручання у систему** – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це (кваліфікується за ст. ст. 361, ст. 361-2, 363-1 КК України); **зловживання пристроями** – навмисне вчинення, без права на це: виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих вище; комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих вище (кваліфікується за ст. 361-1 КК України); **володіння пристроями**, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих вище; комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї

або частини комп'ютерної системи предметом, з наміром їх використання для вчинення будь-якого зі злочинів, перерахованих вище (ст. 361-1 КК України);

- **Правопорушення, пов'язані з комп'ютерами: це підробка, пов'язана з комп'ютерами** – навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти з наявністю наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності та **шахрайство, пов'язане з комп'ютерами** – навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом (кваліфікується за сукупністю ст.ст. 190 та 361 КК України);
- **Правопорушення, пов'язані з дитячою порнографією:**
  а) вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
  б) пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
  в) розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
  г) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;
  д) володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації (кваліфікується за ч. 4, 5 ст. 301 КК України);
- **Правопорушення, пов'язані з порушенням авторських та суміжних прав** (кваліфікується за ст.ст. 176, 177 КК України).

Вивчивши дану Конвенцію та проаналізувавши її відповідно до національного кримінального законодавства, можна зробити висновок про те, що **в національному законодавстві передбачені злочини, суб'єктом яких є особа, що має право доступу до інформації:** ст. 362 "Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї" та ст. 363 "Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється".

Література

1. Кримінальний кодекс України від 05.04.2001 // Голос України від 19.06.2001 – № 107.

2. Спільний наказ МВС, СБУ, ДПА, Держмитслужби, Генеральної прокуратури, Держкомкордону України від 09.01.1997 р. № 3/4/2/5/2/2 “Про затвердження Інструкції про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів” // Офіційний вісник України – 1997 р., № 9, С. 77.
3. Конвенція про кіберзлочинність (ратифіковано із застереженнями і заявами Законом № 2824-IV від 07.09.2005, ВВР, 2006 р., № 5–6, ст.71) // Офіційний вісник України від 10.09.2007 – 2007 р., № 65, С. 107.
4. Постанова Кабінету Міністрів України від 25 березня 1993 року № 220 “Про Національне центральне бюро Інтерполу” // http://zakon1.rada.gov.ua.

О.В. Прохніцький, *ад’юнкт кафедри кримінального права Національної академії внутрішніх справ*

КОМП’ЮТЕРНА ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ ЯК ПРЕДМЕТ ЗЛОЧИНУ

Відповідно до статті 17 Конституції України, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, справою всього Українського народу.

Інформаційні ресурси та інформаційна інфраструктура відіграють дедалі більшу роль у міждержавній боротьбі за світове лідерство і досягнення політичних, економічних та воєнних цілей. Тому, стійке функціонування інформаційної інфраструктури, забезпечення інтересів особи, суспільства і держави у цій сфері перетворюється на важливий чинник збалансованого розвитку будь-якої країни. Усі держави світу намагаються забезпечити правовою охороною власні таємниці. Не є виключенням з цього правила й Україна.

Однак у вітчизняній юридичній літературі недостатньо вирішеним, видається питання щодо відмежування таємної інформації від конфіденційної. Не досягнуто одностайності у вирішенні низки питань, які на нашу думку, мають суттєве значення для кваліфікації діянь, предметом яких є інформація з обмеженим доступом.

Суттєвий внесок у дослідження інформації з обмеженим доступом як предмета злочину зробили, зокрема, такі вчені, як Г.О. Андрощук, Д.С. Азаров, М.К. Галянтич, В.А. Голубєв, В.Д. Гавловський, А.М. Гуз, С.О. Орлов, О.В. Кохановська, М.Й. Коржанський, П.П. Крайнєв, Є.В. Лащук, А.А. Музика, О.К. Мазуренко, П.П. Михайленко, О.Е. Радутний, В.В. Саєнко, О.С. Самойлова, В.Я. Тацій.

Перед тим, як розпочати аналіз комп’ютерної інформації з обмеженим доступом слід надати визначення поняття предмета злочину. У цьому контексті ми схиляємося до концепції Є.В. Лащука, який визначає предметом злочину матеріальні цінності (котрі людина може сприймати органами чуття чи фіксувати спеціальними технічними за-

собами), з приводу яких та (або) шляхом безпосереднього впливу на які вчиняється злочинне діяння [4, с. 8].

Відповідно до Закону України від 2 жовтня 1992 р. "Про інформацію", до таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Слід також наголосити і на тому, що таємна інформація є різновидом інформації з обмеженим доступом. Інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Остання за своїм правовим режимом, може бути двох різновидів – конфіденційна і таємна (ст. 30).

Конфіденційною та таємною може бути також інформація, що, зокрема, може міститися в комп'ютерній мережі і доступ до якої здійснюється лише з дозволу особи, якій вона належить. Кримінальна відповідальність за викрадення, привласнення та вимагання такої інформації передбачена статтями 361^2, 362 КК України.

Так, предметом зазначених злочинів є комп'ютерна інформація з обмеженим доступом, – інформація з обмеженим доступом, що зберігається в електронно-обчислюваних системах (ЕОМ), автоматизованих системах (АС), комп'ютерних мережах або на носіях такої інформації.

З цього приводу, Д.С. Азаров вважає, що поряд із речами матеріального світу предметом злочину необхідно вважати й інші матеріальні утворення (зокрема, комп'ютерну інформацію), впливаючи на які винний завдає шкоди об'єкту чи створює небезпеку заподіяння такої шкоди. Під комп'ютерною інформацією, на його думку, слід вважати відомості про оточуючий світ та процеси, що в ньому відбуваються, які представлені у формі даних, зафіксованих в електронному вигляді [3, с. 9].

Відповідно до ст. 362 КК України передбачена кримінальна відповідальність за "Незаконні дії з інформацією, яка оброблюється в електронно-обчислюваних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї". В свою чергу, відповідно до ст. 361^2 КК України передбачається кримінальна відповідальність за "Несанкціонований збут або розповсюдження інформації з обмеженим доступом яка оброблюється в електронно-обчислюваних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації".

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом (ст. 28 Закону України від 2 жовтня 1992 "Про інформацію"). Виходячи з цього, вважаємо за доцільне об'єднати ст. 361^2 КК України, в ч. 3 ст. 362 КК України та викласти її в такій редакції, "Дії, передбачені частиною першою або

другою цієї статті, вчинені щодо інформації з обмеженим доступом, повторно або за попередньою змовою групи осіб, або якщо вони заподіяли значну шкоду.

Література

1. Конституція України від 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – С. 142.
2. Закон України від 2 жовтня 1992 р. "Про інформацію" // Відомості Верховної Ради. – 1992. – № 48. – С. 650.
3. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. дис … канд. юрид. наук: 12.00.08 / Інституті держави і права ім. В.М. Корецького Національної академії наук України. – К., 2003. – 21 с.
4. Лащук Є.В. Предмет злочину в кримінальному праві України: Автореф. дис. … канд. юрид. наук: 12.00.08 / Київський національний університет внутрішніх справ. – К., 2005. – 20 с.

А.В. Мировська, *ад'юнкт кафедри криміналістики*
Національної академії внутрішніх справ

ОСНОВНІ СУЧАСНІ ЗАХИСНІ ЕЛЕМЕНТИ ГРОШОВИХ ЗНАКІВ

Використання спеціальних знань сприяє ефективності розслідування будь-якого злочину. Особливо це актуалізується при розслідуванні фальшивомонетництва. Адже слідчому необхідно володіти або залучати до сфери кримінального судочинства знання фахівців про захисні елементи банкнот, способи їх підробки, ознаки, що свідчать про підробку тощо. Такі знання не є загальновідомими, здобуваються в результаті освіти за спеціальністю, спеціальної підготовки, досвіду роботи, за своєю природою не відносяться до юридичних, а тому є спеціальними.

Окремий блок спеціальних знань становлять відомості про захисні елементи паперових грошей. Умовно захисні елементи банкнот можна поділити на дві групи: захисні елементи паперу та захисні елементи друку.

Для банкнот використовують спеціальний папір, виготовлений на основі бавовни або льону. Такий папір має характерну фактуру, шурхіт, хрустіння, не люмінесціює в ультрафіолетових променях.

Розмір банкноти чітко визначений, краї рівні. Не допускається виготовлення банкноти із двох склеєних аркушів паперу.

При виготовленні паперу на нього наносять водяні знаки, впроваджують захисну стрічку, захисні волокна та конфетті.

Водяні знаки можуть бути локальними та периферійними; позитивними та негативними, штриховими та тоновими.

Захисна стрічка виготовляється з полімеру, покритого барвником, що має магнітні властивості. Як правило, на захисній стрічці присутній мікротекст. Іноді захисна стрічка покривається барвниками декількох

кольорів, барвником з голографічним ефектом або з люмінесцентними властивостями. Захисна стрічка занурюється у вологий папір при його виготовленні. Вона може повністю знаходитись у товщі паперу або ж бути "пірнаючою".

Захисні волокна (кольорові, безбарвні з люмінесцентними властивостями, комбіновані) роздмухуються струменем повітря над вологим папером у процесі його виготовлення. Саме тому захисні волокна розташовані хаотично, знаходяться на поверхні паперу, кріпляться до нього без клейових речовин.

Конфетті також бувають кольорові, безбарвні з люмінесцентними властивостями, комбіновані, додаються до паперу під час його виготовлення, однак знаходяться у верхніх шарах паперу. Для друку паперових грошей використовується фарба, що має спеціальний хімічний склад.

Для виготовлення банкнот використовують чотири основних способи друку: високий (серія та номер банкноти), глибокий (елементи, які відчутні на дотик), плоский (фонові малюнки, зворотна сторона банкноти), трафаретний (номінал банкноти, який виконаний фарбою OVI, що змінює колір залежно від кута спостереження). Разом з тим, слід зазначити, що за способом друку виготовлення банкнот різних країн може відрізнятися.

Під час друку може застосовуватись райдужний ефект та орловський друк. Захисними елементами також є мікротекст, кіп-ефект, суміщені зображення, антисканерна сітка, ультрафіолетовий та інфрачервоний захист, магнітна карта, кінеграми тощо.

Знання захисних елементів дозволяє виявити підробку банкноти. За способом підробки ведуть обліки фальшивих банкнот, що дозволяє виявити злочинця чи злочинну групу, які займались виготовленням та реалізацією підроблених грошових знаків.

І.М. Попова, *здобувач кафедри криміналістики*
Національної академії внутрішніх справ

ОСОБЛИВОСТІ ПРИЗНАЧЕННЯ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ЕКСПЕРТИЗ У СПРАВАХ ПРО ФІНАНСОВІ ЗЛОЧИНИ

Ефективність досудового розслідування безпосередньо пов'язана з використанням можливостей судових експертиз. З усієї кількості вивчених нами кримінальних справ про фінансові злочини, майже в половині випадків очевидні помилки слідчих на етапах збирання матеріалів для експертних досліджень, призначення експертизи, використання її результатів у доказуванні. Йдеться про потребу кваліфікованого

опрацювання широкого кола нормативних актів, установчих і реєстраційних документів суб'єктів господарювання, бухгалтерської звітності, фінансових розрахунків тощо.

Комп'ютерно-технічна експертиза як самостійний вид експертиз виникла в системі МВС зовсім недавно і на даний час зайняла своє місце в Державному науково-дослідному експертно-криміналістичному центрі МВС України та обласних науково-дослідних експертно-криміналістичних центрах.

Видову класифікацію комп'ютерно-технічної експертизи доцільно розглядати на основі призначення (апаратна, програмна, інформаційна) та використовувати її у вигляді, який відповідає процесам розробки та експлуатації: апаратно-комп'ютерна; програмно-комп'ютерна; інформаційно-комп'ютерна; комп'ютерно-мережева експертиза; комплексні експертизи.

Специфічним є криміналістичне дослідження документів, що виготовлені з використанням комп'ютерних і копіювальних технологій, що останнім часом стає об'єктом пильної уваги криміналістів. Основними завданнями комп'ютерно-технічної експертизи є: встановлення технічного стану комп'ютерної техніки; виявлення інформації, що міститься на комп'ютерних носіях, та визначення її цільового призначення; встановлення відповідності програмних продуктів певним параметрам; встановлення авторства програмного продукту; визначення вартості програмного продукту; визначення вартості комп'ютерної техніки.

Об'єктами комп'ютерно-технічної експертизи є такі: системні блоки комп'ютерів та їх комплектуючі, ноутбуки; периферійні пристрої (принтери, сканери, дисководи, модеми, тощо), комунікаційні пристрої комп'ютерів і обчислювальних мереж; магнітні носії інформації (накопичувачі на жорстких та гнучких магнітних дисках, оптичні диски, флеш-карти пам'яті); електронні записні книжки, пейджери, мобільні телефони та інші електронні носії текстової або цифрової інформації.

Практикою напрацьовані певні вимоги до об'єктів, які направляються на комп'ютерно-технічну експертизу:

- системні блоки комп'ютера та інші пристрої повинні бути упаковані й опечатані таким чином, щоб виключити будь-яку можливість їхнього пошкодження, вмикання в мережу та розбирання;
- у протоколі повинні бути точно вказані місце, час вилучення, а також зовнішній вигляд предметів і документів, які направляються на експертизу;
- при вилученні комп'ютерів та електронних носіїв інформації їх варто упаковувати в поліетиленовий (або полотняний) пакет і далі опечатувати вже сам пакет. Носії інформації також можна упакувати в

картонну чи пластмасову коробку і потім її опечатати. Варто зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їхня кількість). Коробку з носіями та опис помістити до поліетиленового пакету, який потім заклеїти;

- під час перевезення комп'ютерних засобів необхідно вжити заходів щодо запобігання їх механічного пошкодження і взаємодії з хімічно активними речовинами.

Порядок надання об'єктів для дослідження спеціалістом детально регламентовано науково-методичними рекомендаціями з питань підготовки та призначення судових експертиз, затвердженими наказом Міністерства юстиції України № 53/5 від 8 жовтня 1998 р. Для дослідження інформації, яка міститься на комп'ютерних носіях, експертові надається сам комп'ютерний носій, а також комп'ютерний комплекс, до складу якого входить досліджуваний носій. У деяких випадках можна обмежитися наданням тільки комп'ютерного носія. Про можливість проведення цього дослідження слід проконсультуватися з експертом (спеціалістом).

Щоб визначити, які саме об'єкти слід надавати експертові у кожному конкретному випадку, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки.

Під час експертного дослідження нерідко важливо визначити ознаки, обумовлені як технологією виготовлення печатки на документі, так і механізмом нанесення відбитку. При цьому, поряд із класичними питаннями (яким способом виготовлено кліше, яким чином нанесено дослідний відбиток, яким способом нанесено зображення відбитку печатки на документі, чи одним кліше нанесено відбитки на досліджуваних документах, чи нанесено відбиток печатки, зразки відбитків якої надані для дослідження) слідчий повинен ставити перед експертом питання, що вирішуються під час проведення комплексної техніко-криміналістичної і комп'ютерно-технічної експертизи.

О.О. Соловей, *магістр права,*
здобувач кафедри кримінології та кримінально-виконавчого права
Національної академії внутрішніх справ

СУСПІЛЬНА НЕБЕЗПЕКА ДИТЯЧОЇ ПОРНОГРАФІЇ В МЕРЕЖІ ІНТЕРНЕТ

У зв'язку із активними процесами глобалізації та інформатизації сучасного суспільства, новітні комп'ютерні технології, сучасна аудіо- та відеоапаратура спрощують виготовлення та поширення порнографічної продукції. На сьогодні технологічний прорив та ступінь неналежної контрольованості інформаційної телекомунікаційної мережі Інтернет, відсутність її територіальних меж, наявність численних способів ано-

німного розміщення інформації, широка аудиторія користувачів, можливість електронної купівлі-продажу зумовили широке використання віртуального простору представниками порноіндустрії. Такі явища в Україні давно вийшли за межі поодиноких випадків.

На сьогодні в мережі Інтернет діють організовані злочинні групи, що розповсюджують порнографічні матеріали з використанням зображення дітей. Варто також відзначити й те, що безконтрольне розповсюдження дитячої порнографії в мережі Інтернет веде до потенційної небезпеки, оскільки має негативний вплив на свідомість споживачів інформаційних ресурсів, у тому числі на моральне виховання підростаючого покоління.

Основна причина, що сприяє цьому виду злочину полягає в неефективності кримінально-правових та кримінологічних заходів боротьби зі злочинністю у сфері високих технологій, і як наслідок – правозастосовній практиці у боротьбі з виготовленням та обігом дитячої порнографічної продукції в мережі Інтернет.

Труднощі при документуванні злочинів, передбачених ст. 301 КК України, полягають насамперед у проблемах виявлення фактичного місця хостингу порносайтів, встановлення фізичного місця розташування техніки, що була використана для їх створення, реєстрації та редагування (оновлення), а також виявлення осіб, причетних до таких дій.

Так, лише за даними Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, МВС України, за період 2003–2008 років кількість зареєстрованих злочинів, що передбачені ст. 301 КК України (ввезення, виготовлення, збут і поширення порнографічних предметів) постійно збільшувалася: 2003 р. – 235, 2004 р. – 281 (винесено 115 судових рішень), 2005 р. – 366 (винесено 130 судових рішень), 2006 р. – 571 (винесено 191 судових рішень), 2007 р. – 811 (винесено 321 судових рішень). Упродовж 2008 року зареєстровано 956 таких злочинів (винесено 364 судових рішень).

Серед зазначеної загальної кількості кримінальних справ кількість порушених за ст. 301 КК України кримінальних справ, де потерпілими є діти, у 2002 та 2003 роках становила лише по 3 справи, у 2004 – 6, 2005 – 7, 2006 – 6, 2007 – 5 кримінальних справ. Зрозуміло, що навряд чи ці показники відображають реальну небезпеку дитячої порнографії, оскільки дані злочини, у більшості випадків залишаються латентними. Отже, на сьогодні досить складно оцінити реальну кількість дітей в Україні, які стали жертвами порноділків.

Необхідно також зауважити про те, що в кримінальному законодавстві України відсутнє чітке визначення дитячої порнографії, а тому

перед нами постає проблема відмежування її від еротики. Для вирішення цієї проблеми необхідно вдаватися до комплексної експертизи.

За спостереженнями працівників правоохоронних органів, випадки використання дітей в порнобізнесі залишаються невідомими через те, що іноді батьки використовують власних дітей для виготовлення порнопродукції або передають іншим особам своїх дітей для виготовлення такої продукції за що отримують гроші. Водночас реєструються випадки, коли самі підлітки з неблагополучних родин пропонують себе для виготовлення порнографічної продукції через бажання швидко заробити гроші для задоволення власних потреб або навіть для своєї родини.

Виходячи з цього варто відзначити, що мережа Інтернет, як система отримання і розповсюдження інформації, дозволяє анонімно здійснювати злочинну діяльність. Злочинні угруповання широко використовують можливості мережі у своїй суспільно-небезпечній діяльності. Ними створюються відповідні сайти, web-сторінки, які присвячені секс-індустрії, де розміщена реклама порнографічного змісту із використанням зображення дітей.

Враховуючи величезну кількість користувачів Інтернет, на сьогодні, послуги сексуального характеру поставлені на якісно новий рівень. За допомогою мережі Інтернет в режимі-онлайн можна обрати дитину за своїми уподобаннями, переглянути її фото або знайти інформацію відносно фізичних даних, захоплень і навіть почути голос. Якщо відповідної анкети не знайшлося, замовник може відправити повідомлення з необхідними параметрами для індивідуального підбору "товару".

Подальша комп'ютеризація населення України та постійне збільшення користувачів мережі Інтернет дозволяє інтенсивно розвиватися порнобізнесу. За оцінками зарубіжних експертів, один "розкручений" порносайт приносить власникам прибуток до 2 млн доларів США на рік. Дитяча порнографія може використовуватися відвідувачами таких сайтів у різних цілях: для особистого сексуального збудження та задоволення, в комерційних цілях (продажу порноматеріалів), для виправдання своєї поведінки, для створення відповідного "авторитету" в певних колах: кримінальних, в середовищі педофілів, для шантажу дитини, для розбещення чи розпусти, для приниження дитини, отримання викупу тощо.

У мережі Інтернет поширюється до 75 % всієї дитячої порнопродукції. За даними правоохоронних органів, близько 90 % міжнародних пошукових доручень Інтерполу по комп'ютерній злочинності присвячені саме цій проблемі. Світова порнографічна індустрія, знаючи про недосконаліть українського кримінального законодавства, прагне пе-

ремістити свої ресурси дитячої порнографії на територію української частини Інтернету.

Таким чином, можна зробити висновки, що злочини, пов’язані з дитячою порнографією, посягають насамперед на права дитини та на її повноцінне та гідне життя. Комерційна сексуальна експлуатація дітей може призвести до серйозних наслідків у фізичному, психологічному, духовному, моральному та соціальному розвитку підлітків, які можуть зберегтися протягом всього подальшого життя, а часом можуть навіть йому загрожувати.

Секція 3

ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ ТА ВІДМИВАННЮ ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ ЗА ДОПОМОГОЮ ФІНАНСОВИХ ІНСТРУМЕНТІВ, КОМП'ЮТЕРНИХ МЕРЕЖ, БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМ

О.Є. Користін, *д-р юрид. наук, доц.,*
начальник кафедри економічної безпеки
Національної академії внутрішніх справ

ВОЛЬФСБЕРЗЬКІ ПРИНЦИПИ В ЗАПОБІГАННІ ВІДМИВАННЮ КОШТІВ

Порівняно новою в Україні є проблематика протидії відмиванню коштів. Вітчизняне законодавство у цій сфері лише формується. Значним доробком щодо формування ефективної системи протидії відмиванню коштів в Україні є організаційний досвід та нормативно-правове регулювання у розвинених країнах, зокрема, Євросоюзу.

З огляду на такий досвід, для вітчизняних фахівців у сфері протидії відмиванню коштів є достатньо відомими більшість міжнародно-правових актів, міжнародних стандартів. Поряд з цим, заслуговує на увагу ще одна ініціатива у боротьбі з відмиванням коштів, яка була запропонована у жовтні 2000 р. і отримала назву Вольфсберзькі принципи. Вона відрізнялась від багатьох існуючих ініціатив тим, що була запропонована приватним сектором. Вольфсберзька ініціатива – це незобов'язувальний комплекс керівних принципів, що відображають передовий досвід, згідно з якими мають налагоджуватись та підтримуватись зв'язки між приватними банкірами та їх клієнтами [1, с. 262]. Як зазначив Пітер Айген, голова організації Transparency International, з приводу публікації Вольфсберзьких принципів: "Це унікальна подія – небагато людей могли очікувати, що провідна організація з боротьби з корупцією та провідні банки зможуть стати на одну платформу" [2].

На сьогодні більшість ініціатив щодо протидії відмиванню коштів висувалися державним сектором. Той факт, що приватний сектор без примусу з боку органів державного сектора взяв на себе ініціативу створення комплексу принципів щодо протидії відмиванню коштів означає, що ці принципи заслуговують на те, аби бути проаналізованими з

наступним зосередженням на сильних та слабких сторонах кожного з них та можливого використання у подальшому. Зважаючи на те що Вольфсберзькі принципи є ініціативою приватного сектора, хоча їх розробка проводилася під керівництвом членів FATF, ці принципи відповідають вимогам міжнародних стандартів протидії відмиванню коштів. І так як аналіз принципів вимагає більш ґрунтовного підходу (такий аналіз має місце в монографії автора), перш за все, бажаним було б розглянути в основних рисах їх концептуальне підґрунтя.

Для того щоб завершити розробку Вольфсберзьких принципів, потрібно було три роки, а назву вони отримали від назви навчального центру банку United Bank of Switzerland (UBS), де відбувалися перемовини. У процесі брали участь 11 банків, а саме: ABN Amro Bank, Banco Santander Central Hispano, Barclays Bank, The Chase Manhattan Private Bank, Citibank, Credit Suisse Group, Deutsche Bank, Hongkong Shanghai Bank Corporation, JP Morgan, Societe Cenerale та, звичайно, UBS. Крім того, ці принципи підписали Banca Commerciale Italiana та Banca del Gottardo [1, с. 263].

Перелік учасників справляє враження. Слід звернути особливу увагу на те, що до складу учасників ввійшли UBS та Credit Suisse Group, позаяк це дві найважливіші фінансові установи Швейцарії, а Швейцарія, у свою чергу, залишається одним із найважливіших фінансових центрів діяльності приватних банків у світі. Однак доцільно звернути увагу на те, що з-поміж зазначених банків відсутні Merrill Lynch, Morgan Stanley, Goldman Sachs, а також на те, що немає жодного японського або південноамериканського банку. Слід також звернути увагу на те, що із 11 банків, що підписали Вольфсберзькі принципи, більшість були пов’язані (у тій чи іншій формі) з фінансовими скандалами та скандалами, пов’язаними з відмиванням коштів. Наприклад, Citibank допомагав у відмиванні коштів таким людям, як Рауль Салінас де Гортарі, брат президента Мексики Карлоса Салінаса де Гортарі, Мохаммед та Ібрахім Абача, сини президента Нігерії Сані Абача, та президент Габону Омар Бонго [3]. Credit Suisse Group, на додаток до проблем, із якими він зіткнувся впродовж останніх двох років у Японії [3, с. 371], останнім часом піддавався жорсткій критиці з боку швейцарських органів, відповідальних за банківський нагляд, з приводу того, що він прийняв 214 млн дол. США від родини Абача [3, с. 215]. Chase Manhattan Bank був замішаний у скандалі з міддю, що мав місце у 1996 р., який розгорнувся навколо трейдера мідді банку Sumitomo Bank Ясуо Хаманакі [1, с. 263]. На додаток до цього UBS, який є об’єднаною одиницею двох банків, Swiss Bank Corporation та United Bank of Switzerland, був у центрі скандалу, що розгорнувся навколо експропріації банківських рахунків жертв Холокосту [1, с. 263].

Таким чином, не дивно, що після підписання Вольфсберзьких принципів деякі приватні банкіри відразу ж заявили, що це була лише звичайна піарна кампанія [4, с. 112] і що публікація Вольфсберзьких принципів є спробою передбачення вживання урядом подальших заходів, спрямованих на контролювання відмивання коштів, принаймні у сфері приватної банківської діяльності. Останнім часом увага урядових органів до послуг, наданих фінансовими установами, та їх сприйнятливості до відмивання коштів посилилась. Зважаючи на зловживання як у сфері послуг, наданих приватними банками, так і в сфері надання кореспондентських рахунків, що були викриті Конгрессом США, думка, що Вольфсберзькі принципи – просто піарна кампанія, не викликає здивування. Однак, як зауважив інший швейцарський банкір, "нас треба розглядати як складову вирішення проблеми, а не як складову самої проблеми" [5]. Зважаючи на те як тиснуть на банки законодавці, регулятивні органи та працівники правоохоронних органів упродовж останніх кількох років, Вольфсберзькі принципи мають розглядатися як щось більше ніж просто піарна кампанія, про що свідчить більш детальний їх аналіз.

Необхідно зазначити, що важлива проблема, яку мали вирішити саме регулятори фінансового ринку, полягала у тому, як ефективно контролювати роботу банків, їх дочірніх підприємств, та фінансову діяльність, якою вони займаються. Враховуючи надзвичайні складнощі у зазначеному процесі, за основу було взято підхід, відповідно до якого має створюватись гнучка наглядова структура за рахунок того, що банки матимуть можливість розвивати внутрішні механізми контролю ризиків та управління. Вольфсберзькі принципи представляють складову цього гнучкого підходу до регулювання. Вони створили комплекс заходів, прийнятих деякими банками, не тому, що їх примусили регулятивні органи, а добровільно. Вони зосереджуються на контролі та збиранні інформації про діяльність клієнтів для того, аби мати більше можливостей для виявлення підозрілої діяльності. Як комплекс правил про те, як менеджменту належить виконувати цей обов'язок, Вольфсберзькі принципи забезпечують відправну точку для дій у сфері приватних банківських послуг. Як зауважив д-р Айген: "Розмова коротка. Тягар контролю за впровадженням та щоденною дією лежить цілком на банках. Йдеться про їхню репутацію" [2]. Хоча деякі вважають Вольфсберзькі принципи піарною кампанією, у разі їхнього енергійного впровадження вони можуть зробити значний внесок у боротьбу з відмиванням коштів.

У якості доповнення та прикладу реального підходу щодо протидії відмиванню коштів у Вольфсберзьких принципах, зупинемось на 4 принципі (це окремий розділ), який зосереджується на практиці,

пов'язаній із виявленням незвичної або підозрілої діяльності, і наголошує, що "банк повинен мати письмово оформлену політику з виявлення та відстеження незвичної та підозрілої діяльності. Ця політика включає визначення того, що розуміють під словами "незвичний" та "підозрілий", з наведенням прикладів". Далі зазначається, що незвична або підозріла діяльність може включати операції з рахунками або іншу діяльність, яка несумісна з нормами процедури належної пильності, переведення коштів у сумі вище за певний ліміт та операції на кшталт пропускання коштів через рахунок або отримання та переведення коштів далі. Перелік не є вичерпним внаслідок динамічного характеру процесу відмивання коштів. У тій мірі, в якій ті, хто відмиває кошти, продовжуватимуть розробляти нові методи відмивання коштів, змінюватиметься і визначення підозрілої діяльності. Тут буде корисним наголосити на важливості ідеї зворотного зв'язку. Відмивання коштів буде успішно контролюватися тоді, коли банки, регулятори та правоохоронні органи будуть працювати разом, допомагаючи одне одному. Корисним буде створення системи взаємодопомоги, коли банки вимагатимуть зворотного повідомлення про те, чи виявилася корисною інформація, яку вони надали регуляторам та правоохоронним органам. Тільки завдяки належному зворотному зв'язку банки зможуть підтримувати сучасну програму відповідності. Як частина процесу може бути важливим, аби регулятори та правоохоронні органи повідомляли банкам про операції та діяльність, які вони вважають підозрілими. Стосовно цього корисною є діяльність щодо визначення типології, методів та тенденцій відмивання коштів, а також доповіді на ці теми [1, с. 276].

Таким чином, ми бачимо яскравий приклад ініціативи саме учасників фінансового ринку до взаємодії з правоохоронними органами щодо протидії відмиванню коштів.

Література

1. Hinterseer K. Criminal Finance. The Political Economy of Money Laundering in a Comparative Legal Context // Kluwer Law International, 1995.
2. Peter Eigen. Opening Statement on the Release of New Anti-Money Laundering Guidelines at a Press Conference on October 30, 2000(October 30. 2000).: Ел. ресур.: <htt://www.transparency.org>.
3. Stessens G. Money Laundering: a new international law enforcement model. – Cambridge University Press., 2000. – 460 p.
4. Міжнародна банківська справа та відмивання коштів: Матеріали міжнародного семінару (м. Київ, 15–19 лютого 1999 р.). – Глінко, Федеральний правоохоронний навчальний центр, 1999. – 230 с.
5. Gary Kochberg, "Getting Your Principles Right – ON New Regulations to Combat Money Laundering" (November 8, 2000).: Ел. ресур.: htt://www.accountancyage.com.
6. Користін О.Є. Відмивання коштів: теоретико-правові засади протидії та запобігання в Україні. Монографія. / О. Є. Користін // Київ. нац. ун-т внутр. справ. – К., 2007. – 448 с.

О.Б. Жихор, *д-р екон. наук, проф., завідувач кафедри фінансів*
Харківського інституту банківської справи
Університету банківської справи НБУ;
Н.В. Кузьминчук, *канд. екон. наук, доц., докторант*
Національного технічного університету "ХПІ"

МЕТОДИКА КОМБІНОВАНОЇ ОЦІНКИ ОБСЯГІВ ПРИХОВАНОЇ ВАЛОВОЇ ДОДАНОЇ ВАРТОСТІ ПРОМИСЛОВОСТІ ХАРКІВСЬКОГО РЕГІОНУ

В Україні одним з найбільш поширених економічних злочинів є і залишається ухилення від сплати податків, зборів та інших обов'язкових платежів. На даний час є підстави стверджувати, що ухилення від платежів до бюджету стало нормою поведінки багатьох керівників суб'єктів оподаткування. В результаті проведення тіньових операцій держава недоодержує належних їй коштів, а у суспільстві створюється економічний базис організованої злочинності. Несплата податків досягає таких масштабів, коли вона із економіко-соціальної проблеми поступово перетворюється в проблему економічної безпеки держави, зокрема її регіонів.

За оцінками експертів Міністерства економіки України в "тіні" перебуває понад 120 млрд. грн., а за даними Департаменту економічної стратегії Міністерства економіки за І півріччя 2006 року рівень "тінізації" економіки склав 50 % [10, с. 9]. Причому, найбільша частка у структурі тіньової економічної діяльності, розрахованої фінансовим методом, належить промисловості, що пояснюється її значним внеском до ВДВ економіки (28 %) за рівня тінізації у 22 % [3, с. 58].

На сьогоднішній день розроблено ряд науково-методичних рекомендацій до визначення та оцінки обсягів тіньової економіки. Серед відомих українських та російських вчених, які внесли значний вклад у розвиток цієї проблеми, слід відмітити наукові праці В. Базилевича, І. Мазур [1], В. Бородюка, О. Турчинова, Т. Приходько [2], З. Варналія [3], В. Вишневського [4–5], Г. Нестеренко [7], С. Нікітіна [8], Ю. Прилипко, Л. [9], Харазішвілі Ю.М. [11] та ін. Але науково-методологічну базу для аналізу й прогнозування тіньової економіки не можна вважати створеною в повному обсязі.

Метою роботи є узагальнення досвіду оцінок економічної діяльності в тіньовому секторі та на цій основі розробка методики оцінки обсягів тіньової економіки з метою визначення втрат податкового потенціалу регіону.

Вибір методів оцінки обсягів тіньової економіки залежить від кожної конкретної ситуації. В умовах відсутності статистичного матеріалу краще комбінувати кілька методів [1, с. 41]. Виходячи з цього автором

пропонується методика комбінованої оцінки обсягів (по роках) прихованої валової доданої вартості у промисловості Харківської області за період з 2002 по 2007 роки, яка ґрунтується на фінансовому та монетарному методах, викладеними у роботах [6, 9].

Застосування цих методів одночасно, обумовлено тим, що фінансовий метод надає можливість отримувати лише оцінки зміни прихованої валової доданої вартості (ВДВ), у зв'язку з чим, виникає необхідність визначення обсягів тіньової економіки у певному базовому році. Монетарний метод (метод Гутмана) виходить з того, що збільшення попиту на готівку, яка перебуває в обігу поза банківськими рахунками, означає зростання обсягів тіньових операцій, і навпаки. Припускається відсутність тіньової економіки в базовому періоді За базовий період приймається 1-й квартал 1992 р.

Слід відзначити, що деякі дослідники відзначають недосконалість монетарного методу. Зокрема недостатньо обґрунтованим вважається припущення, що всі зміни у співвідношенні готівки і вкладів відбуваються тільки під впливом тіньової економіки. На це співвідношення істотно впливають інфляція, податкова система, зміна реального доходу на душу населення, гранична схильність до заощаджень, рівень розвитку фінансових послуг та ін. [11, с. 71]. Ці міркування обумовили вибір фінансового методу у якості основного. Застосування монетарного методу в доповнення до фінансового – обумовлено тим, що фінансовий метод надає можливість отримувати лише оцінки зміни прихованої ВДВ, у зв'язку з чим виникає необхідність визначення обсягів тіньової економіки у певному базовому році (у нашому випадку для 2002 року).

За розрахунками, виконаними на основі монетарного методу, частка тіньового сектора у Харківському регіоні на протязі 2002 року становила близько 36 %. Виходячи з припущення, що частка прихованої ВДВ у загальному обсязі ВДВ є приблизно однаковою за всіма видами діяльності, було прийнято, що частка ВДВ, що відповідає прихованому виробництву (робіт, послуг) у промисловості Харківського регіону в 2002 році, також складала величину 36 %. Відповідно до цього обсяг a_2^0 прихованої ВДВ у промисловості Харківської області у 2002 році дорівнював 2,703 млн. грн.

У табл. 1 наведено результати розрахунків обсягів прихованої ВДВ у промисловості Харківської області за період з 2003 по 2007 роки, які були виконані на основі фінансового методу.

Таблиця 1

Динаміка оцінки частки офіційної ВДВ у загальному обсязі ВДВ

Показник	2002 $t = 0$	2003 $t = 1$	2004 $t = 2$	2005 $t = 3$	2006 $t = 4$	2007 $t = 5$
Величина ВДВ, що відповідає офіційно проведеним агентом операціям, млн. грн.	7,535	9,531	12,541	14,733	18,401	22,096
Обсяг ВДВ, що відповідає прихованому виробництву (робіт, послуг), млн. грн.	2,703	3,208	4,043	5,049	4,683	6,886
Частка офіційної ВДВ у загальному обсязі ВДВ	0,736	0,748	0,756	0,745	0,797	0,762

Як видно з табл. 1, по промисловим підприємствам Харківського регіону відбувається поступове зростання обсягу ВДВ, що відповідає прихованому виробництву (робіт, послуг). Все це не сприяє покращенню іміджу регіону та його конкурентоспроможності. Тому першочерговими завданнями зменшення рівня тінізації є поглиблення управління економічними процесами в регіоні з боку місцевих органів влади шляхом реалізації низки заходів щодо протидії тінізації.

Висновки. Отримані результати досліджень дають змогу зробити такі висновки. Відмінною рисою та головною перевагою запропонованої автором методики розрахунку обсягів тіньової економіки є те, що вона дозволяє розраховувати обсяги тіньової економіки у абсолютних величинах. Розроблений підхід до визначення обсягів тіньової економіки регіону може використовуватися при обчисленні втрат дохідної частини бюджету від тіньової економіки.

Література

1. Базилевич В. Методичні аспекти оцінки масштабів тіньової економіки / В. Базилевич, Мазур І. // Економіка України. – 2004. – № 8. – С. 36–44.
2. Бородюк В. Методи розрахунку обсягів тіньової економіки / В. Бородюк, О. Турчинов, Т. Приходько // Економіка України. – 1997. – № 5. – С. 24–34.
3. Варналій З. Шляхи детінізації економіки України та її особливості / З. Варналій // Банківська справа. – 2007. – № 2. – С. 56–66.
4. Вишневский В. Уклонение от уплаты налогов и рациональный выбор налогоплательщика / В. Вишневский, А. Веткин // Вопросы экономики. – 2004. – № 2. – С. 96–108.
5. Вишневський В. Ухилення від сплати податків: моделювання вибору та дій економічного суб'єкта / В. Вишневський, А. Вєткін // Економіка України. – 2004. – № 1. – С. 9–15.
6. Методика розрахунку обсягів тіньової економіки: затверджено Наказом Міністерства економіки України № 222 від 27.06.2006 р. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0833-06#top.

7. Нестеренко Г. М. Моделювання у моніторингу тіньової економіки [Електронний ресурс] / Г. М. Несторенко. – Режим доступу: http://nc.ufei.ukrsat.com/ Kyrsi % 202003/tezi/images_tezi/025.htm.
8. Никитин С. Теневая экономика и налогообложение / С. Никитин, М. Степанова, Е. Глазова // Мировая экономика и международные отношения. – 2005. – № 2. – С. 24–30.
9. Прилипко Ю. Методичні рекомендації щодо інтегральної оцінки обсягів тіньової економіки / Ю. Прилипко, Л. Мусіна, Т. Кваша // Экономика Украины. – 2005. – № 6. – С. 37–44.
10. Смітюх Г. Демократична легалізація тіньових доходів – вимога часу / Г. Смітюх // Урядовий кур'єр. – 2007. – № 12.– С. 9.
11. Харазішвілі Ю. М. Ресурсний потенціал і тіньова економіка регіонів України / Ю. М. Харазішвілі // Банківська справа. – 2006. – № 4. – С. 67–78.

А.Л. Чернявський, *канд. юрид. наук, завідувач кафедри правознавства Севастопольського інституту банківської справи Української академії банківської справи НБУ*

ПРАВОВІ АСПЕКТИ УЧАСТІ УКРАЇНИ У МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ У СФЕРІ БОРОТЬБИ З ЛЕГАЛІЗАЦІЄЮ (ВІДМИВАННЯМ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Ефективність національних систем запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, значною мірою залежить від дієвості відповідних міжнародно-правових механізмів. Міжнародне співробітництво у боротьбі з легалізацією (відмиванням) доходів здійснюється на двосторонньому та багатосторонніх рівнях, при чому основною формою співробітництва в цій сфері є участь держав у діяльності спеціалізованих міжнародних організацій, зокрема Спеціальної комісії з проблем відмивання грошей (FATF) [2, с. 79]. Головними напрямами діяльності FATF є розробка системи заходів, спрямованих на боротьбу з відмиванням грошей, прийняття відповідних рекомендацій та надання технічної допомоги державам, а також проведення інспекційних перевірок у державах-членах FATF з метою оцінки стану справ у галузі боротьби з відмиванням грошей.

Основними формами міжнародного співробітництва у боротьбі з легалізацією доходів є обмін інформацією про виявлені ознаки відмивання грошей та надання правової допомоги у кримінальних справах, пов'язаних з легалізацією доходів.

Відповідно до ст. 22 Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму" в редакції від 18.05.2010 [3] державними

органами, на які покладається реалізація міжнародного співробітництва у сфері запобігання та протидії легалізації (відмиванню) доходів, є:

- Державний комітет фінансового моніторингу – щодо обміну з відповідними органами іноземних держав інформацією про фінансові операції, що підлягають моніторингу;
- Міністерство юстиції України – щодо виконання судових рішень, які стосуються конфіскації доходів, одержаних злочинним шляхом;
- Генеральна прокуратура України – щодо вчинення процесуальних дій у межах розслідування кримінальних справ щодо легалізації (відмивання) доходів, одержаних злочинним шляхом, або фінансування тероризму.

Таке розмежування завдань та предметної компетенції державних органів щодо міжнародного співробітництва у сфері запобігання та протидії легалізації (відмиванню) доходів хоча і виглядає достатньо логічним, проте далеко не повною мірою відповідає існуючим механізмам міжнародно-правової боротьби зі злочинністю.

По-перше, зазначене вище розмежування компетенції Міністерства юстиції України та Генеральної прокуратури України не відповідає нормам ряду міжнародних договорів України про правову допомогу. Так, відповідно до договорів про правову допомогу, які укладалися Україною у перші роки незалежності, наприклад, у договорах з Молдовою (1993 р.), Литвою (1994 р.), Латвією (1995 р.), Естонією (1995 р.), Грузією (1995 р.) тощо, органами, які надають правову допомогу у кримінальних справах, визначалися одночасно Генеральна прокуратура України та Міністерство юстиції України без якого б то не було розмежування повноважень між ними. У новіших міжнародних договорах України про правову допомогу у кримінальних справах, наприклад, з Панамою (2003 р.) чи Єгиптом (2004 р.) органами, на які покладається надання правової допомоги іншим державам, визначаються Міністерство юстиції України щодо запитів судів і Генеральна прокуратура України щодо запитів органів досудового слідства. Крім того, не слід забувати, що механізм надання правової допомоги у кримінальних справах у відносинах з окремими державами визначається ще радянськими міжнародними договорами, щодо яких Україна визнала своє правонаступництво. Зокрема, Договір про правову допомогу між СРСР та Фінляндію 1978 р. чітко визначає, що питання про надання правової допомоги вирішуються виняткова дипломатичним шляхом.

Враховуючи це, може виникнути ситуація, коли при зверненні до України іншої держави про надання правової допомоги у кримінальній справі, пов’язаній з відмиванням доходів, одержаних злочинним шляхом, Генеральна прокуратура не зможе надати правову допомогу, оскільки це суперечить чинному міжнародному договору, а Міністерство

юстиції не зможе зробити те ж саме, оскільки це суперечить Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму".

По-друге, співробітництво у боротьбі з відмиванням грошей здійснюється також і під егідою Міжнародної організації кримінальної поліції (Інтерполу), у складі якого утворено Суб-директорат з питань фінансових злочинів та злочинів з використанням високих технологій [1]. Серед завдань, що покладаються на Суб-директорат, є і обмін інформацією, пов'язаною з відмиванням (легалізацією) доходів, одержаних злочинним шляхом. Україна як член Інтерполу повинна брати участь у співробітництві у боротьбі з відмиванням грошей і в межах вказаного Суб-директорату, проте чинне національне законодавство не дозволяє організувати на належному рівні обмін інформацією про відмивання грошей з органами Інтерполу. По-перше, ст. 22 Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму". дозволяє Держфінмоніторингу передавати інформацію про ознаки легалізації (відмивання) доходів лише відповідним органам фінансового моніторингу іноземних держав, а не міжнародним організаціям, в т.ч. і Інтерполу. По-друге, в межах Інтерполу здійснюється співробітництво між органами кримінальної поліції різних держав, в той час як органи внутрішніх справ України не наділені повноваженнями у сфері боротьби з відмиванням грошей.

Як бачимо, чинне законодавство України та ряд укладених нею міжнародних договорів про правову допомогу у кримінальних справах не дозволяють Україні повністю використати існуючий потенціал міжнародного співробітництва у сфері боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом. В свою чергу, це зумовлює необхідність внесення до законодавства України таких змін, які б чітко і без протиріч з уже укладеними міжнародними договорами визначили б компетенцію Державного комітету фінансового моніторингу, Генеральної прокуратури України, Міністерства юстиції України та Міністерства внутрішніх справ України у сфері боротьби з легалізацією (відмиванням) доходів, одержаних злочинним шляхом.

Література

1. Качка Т. Боротьба з відмиванням грошей / Качка Т. [Електронний ресурс]. – Режим доступу: www.eclc.gov.ua/projects.money_laundering – Заголовок з вікна екрану.
2. Киевец Е. Роль международных специализированных организаций по борьбе с отмыванием денег (на примере FATF) / Киевец Елена Валериевна // Підприємництво, господарство і право. – 2003. – № 7. – С. 79.
3. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму: Закон України в редакції від 18.05.2010 р. // Відомості Верховної Ради України. – 2010. – № 29. – Ст. 1000.

Д.М. Павлов, *канд. юрид. наук, доц.,*
заступник начальника кафедри економіко-правових дисциплін
Національної академії внутрішніх справ

ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ КОШТІВ, ЗДОБУТИХ ЗЛОЧИННИМ ШЛЯХОМ, З ВИКОРИСТАННЯМ СИСТЕМИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ЧЕРЕЗ ОФШОРНІ ЮРИСДИКЦІЇ

Як відомо, на фінансових ринках глобалізація допомогла здійснити прорив кордонів, що були властиві національним фінансовим ринкам у минулому, і призвела до створення інтегрованої всесвітньої фінансової системи, що працює 24 години на добу. Для всіх країн ці процеси забезпечували підвищення рівня інвестицій, створення робочих місць і передачу технологій, навичок і знань, що конче важливо для країн із бідними національними сировинними запасами, оскільки давали широкі можливості для мобілізації ресурсів і підтримки стратегічного розвитку [1]. Все разом це надало переваги не тільки учасникам легальної економіки, але й її нелегального сектора. Використання у нелегальних схемах офшорних юрисдикцій ускладнює моніторинг переміщення коштів. Цей процес також включає зміщування "законних" та "незаконних" прибутків, використання накладних та акредитивів на неіснуючі поставки, перекази на підставні фірми тощо. В останні роки багато все активніше використовуються новітні технологій (системи електронного зв'язку, мережа "Інтернет") при відмиванні коштів, відбувається розвиток нового напряму кіберзлочинності. Наприклад, в багатьох випадках реєстрація компаній, включаючи фінансово-кредитні установи, в офшорах здійснюється через Інтернет.

Кримінальним структурам, які відмивають кошти, процеси, викликані глобалізацією та інтеграцією фінансових ринків, особливо технологічними нововведеннями, дозволили працювати з більшою результативністю і прибутковістю. Зокрема, технологічні нововведення (розвиток електронних платіжних систем, комп'ютерізація банківської діяльності) дали можливість запроваджувати більш складні та витончені схеми легалізації злочинних доходів, але при цьому вони лишались гнучкими й адаптованими. Такі нововведення також підвищили швидкість виконання угод, що дозволило збільшити кількість серійних трансакцій, за допомогою яких особи, котрі відмивали кошти, одержали можливість вибудовувати досі небачену за складністю систему взаємних прихованих розрахунків. Вони також підвищили можливості спілкування, що дозволило проводити трансакції на території більшого числа юрисдикцій, максимально збільшуючи, таким чином, легальні перешкоди на шляху проведення розслідування. Водночас, інтеграція

фінансових ринків спричинює значне зростання обсягу інформації в їхніх межах. Відтак, були створені фінансові інструменти і стратегії, збільшилась загальна вигідність на фінансових ринках. У свою чергу, це дозволяє з легкістю засновувати і ліквідовувати підприємства, що забезпечували існування систем стосовно легалізації злочинних доходів, а підвищення конкуренції знизило витрати на виконання відповідних трансакцій [1]. Як зазначає професор Вільям Гілмор: "Сучасні технології дали новий стимул не тільки для законної торгівлі та комерції, але також для підприємств нелегального бізнесу. Таким чином, масовий розвиток засобів комунікації полегшив контакти зі співучасниками в інших країнах і на інших континентах, сучасна банківська система полегшила здійснення міжнародних злочинних трансакцій, а сучасна революція в електроніці дала злочинним групам доступ до нових інструментів, що дозволяють викрадати мільйони і відмивати величезні незаконні доходи" [2, 14].

Розглядаючи проблематику легалізації коштів із використанням офшорних юрисдикцій, маємо звернутися до визначення категорії "офшор". У багатьох енциклопедичних довідниках міститься таке визначення: "офшор (англ. off-shore – той, що знаходиться на відстані від берега, поза територією держави) – території, що надають пільговий режим (зниження податків, звільнення від валютного контролю тощо) для фінансово-кредитних операцій з іноземними учасниками та в іноземній валюті" [3]. В більшості іноземних джерел не вживається термін "офшорна зона", а використовується поняття offshore financial centre – офшорний фінансовий центр, offshore banking (centre) – офшорний банківський бізнес (центр), bank haven – банківське сховище і інше. Все разом їх об'єднує одна назва offshore jurisdiction – офшорна юрисдикція.

У контексті фінансових трансакцій термін "офшор" належить до трансакцій, що здійснюються між нерезидентами. Відповідно до даного визначення офшорні трансакції можуть мати місце в будь-якій юрисдикції, але в результаті фіскальних правил і правил щодо таємності деякі юрисдикції приваблюють велику кількість офшорних трансакцій і офшорних банків і, таким чином, стають офшорними фінансовими центрами. Все це зводиться до того, що ті, хто легалізує злочинні доходи, нерідко використовують офшорні фінансові центри для приховування такого характеру доходів або для легалізації їх з метою ухилення від оподаткування [3].

В останній час інші країни приймали закони про банківську таємницю на зразок швейцарських, що зумовило виникнення конкуренції у сфері залучення міжнародних капіталів. Багато країн – податкових

сховищ розглядають фінансовий бізнес в якості відносно стабільного джерела доходів і активно розвивають його, проводять політику залучення фінансового бізнесу. Барбадос, наприклад, нещодавно прийняв банківське законодавство для покращення своєї конкурентоспроможності в якості фінансового центру. Багами почали дуже агресивну кампанію для того, щоб стати центром реєстрації банків, страхових компаній і суден. Серед юрисдикцій, які гарантують режим фінансової таємниці, найшвидше розвиваються Кайманові острови, які перетворились в одне з найкрупніших податкових сховищ світу. Сьогодні там зареєстровано біля 18 000 корпорацій, що перевищує кількість місцевих мешканців, і рахується, що є телексний апарат на кожного чоловіка, жінку і дитину на острові Гранд Кайман. За офіційними даними уряду Каймановых островів через конфіденційні банківські рахунки цієї держави щорічно проходять близько 10 мільярдів доларів.

Такий швидкий розвиток офшорної індустрії світу був обумовлений низкою причин, основною з яких є посилення процесів глобалізації у світовій економіці. Основа зародження даного процесу лежить у розвитку науково-технічного прогрессу. Розгортання процесу глобалізації в сфері міжнародних фінансових, операцій також зіграло важливу роль, пов'язану з тим, що сучасний валютний ринок не знає ні просторових, ні часових меж. Більше того, вільне переміщення фінансових коштів у просторі й часі відбувається в рамках єдиної системи, що істотно спрощує доступ інвесторів до фінансових ринків. Таким чином, виникнення всесвітнього чітко організованого ринку валюти й фінансових інструментів, розвиток системи електронних платежів технічно створило можливість використання офшорних зон у процесах руху капіталів. Крім того, залучення в дані процеси компаній, створених в офшорних зонах, дозволило суттєво збільшити рентабельність бізнесу й заощадити на операційних витратах [1].

Прискорення НТП позначилася й на всесвітньому поширенні й здешевленні засобів зв'язку. Це зробило можливим підтримку необхідних контактів між офісами в різних частинах світу як всередині однієї компанії, так і між різними організаціями, розширило діапазон економічної діяльності й комерційних операцій, що не вимагають безпосередніх контактів між сторонами, дозволило реєструвати компанії без необхідності особистої присутності на реєстрації, і спростило процес ведення справ від імені компанії в момент знаходження в протилежній частині світу. І, нарешті, стало можливим здійснювати діяльність будь-якої компанії в буквальному значенні поза просторовими рамками – за допомогою Всесвітньої інформаційної системи [3].

Ефективна боротьба з легалізацією вимагає удосконалення законодавства, зокрема пов'язаного з розкриттям банківської таємниці. Нагальною потребою сьогодення є спрощення процедури доступу правоохоронних органів до інформації, яка становить банківську таємницю, розвиток фінансового моніторингу. Акцент має бути зроблений на відстеженні руху коштів на щойно відкритих рахунках та впровадженні політики градації клієнтів банку в залежності від ступеню ризику участі у схемах, спрямованих на легалізацію коштів, здобутих злочинним шляхом. Крім того, існує потреба Такі заходи сприяють більш ефективному виявленні "брудних" грошей в момент їх обігу у банківських розрахункових системах.

В Україні боротьба з комп'ютерною злочинністю, здійснюється службами протидії комп'ютерним злочинам, які функціонують у системі МВС (основна робота виконується підрозділами ДСБЕЗ) та у Службі безпеки України. Поряд з цим, існує потреба у створенні відповідних підрозділів у складі Державної податкової адміністрації. Крім того, на думку автора, існує потреба у внесенні змін до Закону України "Про банки і банківську діяльність" та у проект Податкового кодексу з метою формування правових засад протидії злочинам, які здійснюються із використанням комп'ютерних мереж і спрямовані на легалізацію коштів через офшорні юрисдикції.

Література

1. Павлов Д.М., Користін О.Є. / Національні фінансові системи в умовах глобалізації: Монографія / За аг. Ред.. проф. Лютого І.О. – м. Івано-Франківськ: Галицька академія, 2008. – 308 с. – Розділ 3.2. – с. 209–228.
2. Gilmore W. International Initiatives in the Field of Money Laundering. – International Banking and Financial Law, 1995.
3. Галкін І.Г. Організаційно-правові засади податкового планування з використанням зон зі спеціальним режимом оподаткування: дис... канд. юрид. наук: 12.00.07 / Київський національний ун-т внутрішніх справ. – К., 2006. – 207 арк.
4. Користін О.Є. Відмивання коштів: теоретико-правові засади протидії та запобігання в Україні. Монографія. Київ. Нац. Ун-т внутр. Справ. – К., 2007. – 448 с.

О.Б. Сахарова, *головний науковий співробітник*
лабораторії проблем правового забезпечення
діяльності органів внутрішніх справ
Державного науково-дослідницького інституту МВС України

ВИКОРИСТАННЯ ЦІННИХ ПАПЕРІВ ЯК СПОСІБ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Використання фінансової системи з метою легалізації (відмивання) доходів, одержаних злочинним шляхом (далі – легалізація (відмивання) доходів), є серйозною перешкодою стабільного розвитку економіки та

загрозою національній безпеці України. Злочинна діяльність з легалізації (відмивання) доходів завдає значної шкоди нормальному функціонуванню фінансово-господарського механізму держави.

Аналіз найпоширеніших способів легалізації доходів у фінансовій системі України за допомогою використання цінних паперів дозволяє узагальнити такі основні типові схеми вчинення цього злочину.

I. Виведення капіталу за кордон з використанням цінних паперів здійснюється таким шляхом:
   1) вітчизняне акціонерне товариство випускає акції;
   2) компанія-нерезидент придбаває випущені акції за низькою ціною;
   3) нерезидент продає ці акції резиденту за ціною, що у багато разів перевищує ціну купівлі;
   4) резидент переказує грошові кошти на рахунки компанії-нерезидента за кордоном.

У результаті безпідставно виводяться значні суми валютних цінностей за кордон з наступним отриманням "відмитого" злочинного доходу за межами країни. Зазначена схема легалізації злочинно одержаних коштів здійснюється за участі банківської установи, яка забезпечує весь комплекс розрахунків у ході проведення зазначених операцій (від надання кредитів, авалювання та випуску векселів до отримання та конвертації валюти за кордоном).

II. Легалізація доходів (конвертація валюти) за допомогою цінних паперів (векселів та ощадних сертифікатів). До найбільш поширених схем конвертації валюти відносяться:
   1) використання ощадних сертифікатів на пред'явника (підприємство придбаває сертифікат у банку, передає його фізичній особі, яка його погашає у банку);
   2) використання доміцильованих векселів (підприємство вносить грошові кошти на рахунок у банку, виписує доміцильований вексель, розраховується останнім з фіктивною фірмою нібито за поставлені товари, фіктивна фірма погашає вексель у банку);
   3) здійснення купівлі іноземної валюти із застосуванням валютних ощадних сертифікатів.

Як правило, на практиці застосовується комбінація цих методів конвертації валюти.

III. Легалізація доходів на основі виписки простих векселів та їх подальшого перепродажу з дисконтом через торговців цінними паперами. Схема вчинення зазначеного злочину полягає у наступному:
   1) організатор легалізації доходів виписує на користь фірми "А" простий вексель як оплату за поставлені товари;
   2) фірма "А", у свою чергу, передає цей вексель за індосаментом фірмі "В" як оплату за отриманий кредит;

3) фірма “В” укладає з торговцем цінними паперами договір комісії про продаж векселя за рахунок комітента;
4) торговець цінними паперами продає вексель фізичній особі з великим дисконтом: за ціною у декілька тисяч разів менше за його суму;
5) фізична особа пред’являє вексель до сплати організатору легалізації доходів. У результаті “відмиті” гроші конвертуються у готівку та легалізуються.

До інших операцій з цінними паперами і похідними фінансовими інструментами, пов’язаних з відмиванням злочинно одержаних доходів, можна віднести:

- легалізацію капіталу, незаконно здобутого на території України або за її межами, шляхом купівлі резидентами через підприємства, зареєстровані в офшорних зонах, інших країнах і територіях із спрощеною системою реєстрації або пільговим оподаткуванням, ліквідних акцій українських підприємств;
- регулярне укладення підприємством строкових угод або використання інших похідних фінансових інструментів (деривативів – опціонів, ф’ючерсів, форвардів), які не передбачають поставки базового активу, за операціями з одним або кількома контрагентами, результатом чого є постійний прибуток або постійні збитки цього підприємства протягом значного часу;
- разовий продаж (купівлю) підприємством великого пакета цінних паперів, що вільно не обертаються на організованому ринку, за цінами, істотно відмінними від ринкових, при цьому підприємство не є професійним учасником ринку цінних паперів і цінні папери не були йому передані в погашення простроченої заборгованості контрагента;
- отримання злочинно одержаних коштів при здійсненні незаконних фінансово-господарських операцій та їх легалізацію шляхом придбання цінних паперів у інвестиційній компанії;
- легалізацію коштів через купівлю акцій підприємств переробних галузей, а також блокуючих пакетів акцій приватизованих підприємств, які залишилися у власності держави, з переведенням цих акцій у розпорядження підконтрольних структур;
- укладання угод підприємства з однією і тією ж стороною щодо купівлі, а потім продажу тих самих цінних паперів.

З метою своєчасного виявлення фактів легалізації доходів під час проведення операцій з цінними паперами і похідними фінансовими інструментами слід звернути посилену увагу на такі документи:

- строкові угоди (опціонні, ф'ючерсні, форвардні), а також строкові угоди, які не передбачають поставки базового активу (товарів, валюти, цінних паперів), за якими підприємство протягом значного часу отримує постійний прибуток чи постійні збитки;
- разові угоди підприємства (не торговця цінними паперами) щодо купівлі-продажу великого пакета цінних паперів за цінами, істотно відмінними від ринкових;
- угоди підприємства з однією і тією ж стороною щодо купівлі, а потім продажу тих самих цінних паперів тощо.

Крім того, доцільно звернути увагу на проведення угод купівлі-продажу цінних паперів на пред'явника.

З метою легалізації доходів також можуть використовуватися так звані фіктивні ("дружні", "зустрічні", "бронзові" ("дуті")) векселі, ознаками яких є:

1) їх видача не пов'язана з реальним переміщенням товарних чи грошових цінностей;
2) їх безнадійність (відсутність у вексельному зобов'язанні законної основи боргу, реальної економічної підстави видачі фіктивного векселя, майнового забезпечення боргу). Підкреслимо, що відповідно до ст. 4 Закону України "Про обіг векселів в Україні" від 05.04.2001 дозволено видавати векселі лише для оформлення грошового боргу за фактично поставлені товари, виконані роботи, надані послуги.

Проблемними питаннями з виявлення фіктивних векселів є відсутність інфраструктури з накопичення даних щодо опротестованих векселів та механізму централізованого документального контролю за видачею, індосацією, акцептуванням, доміциляцією та погашенням векселів.

З метою своєчасного упередження злочинів, що вчиняються за допомогою виписування фіктивних векселів, у процесі легалізації (відмивання) доходів доброчесним суб'єктам господарської діяльності необхідно:

1) вивчити ділові відносини векселедавця і векселедержателя (у випадку переказного векселя – трасанта, трасата і ремітента): родичі, члени (пайовики) одного господарського товариства, друзі, сторони довготривалих господарських зв'язків тощо;
2) з'ясувати такі обставини, що свідчать про високу ймовірність використання в економічних відносинах фіктивних векселів:
   а) якщо два векселі, виставлені двома юридичними особами один на одного або акцептовані ними, пропонуються для врахування

в одному і тому ж самому банку, незалежно від того, чи пропонують ці векселі векселедержатель (ремітент) і векселедавець (трасант, трасат) або яка-небудь стороння юридична особа, що врахувала ці векселі;

б) якщо дві юридичні особи один на одного виставили векселі з практично однаковими строками і сумами сплати за ними;

в) якщо дві юридичні особи виписали один на одного векселі, в яких строки і суми сплати не збігаються, проте ці юридичні особи виступають попеременно то векселедавцем, то векселедержателем.

Література

1. Закон України від 05.04.2001 р. № 2374-ІІІ "Про обіг векселів в Україні".
2. Черкасов Ю.Е., Баліна С.Н., Сахарова О.Б., Близнюк І.Л. Типові способи легалізації (відмивання) доходів, одержаних злочинним шляхом, та заходи щодо протидії їй. – К.: Національна академія внутрішніх справ України, 2005. – 28 с.
3. Камынин И. Противодействие легализации преступных доходов с учетом рекомендаций ФАТФ // Законность. – 2005. – № 4. – С. 18–22.

С.С. Чернявський, *канд. юрид. наук, ст. науковий співробітник,*
начальник наукової лабораторії
проблем запобігання та розкриття тяжких злочинів
Національної академії внутрішніх справ

ДОСВІД ЄВРОПЕЙСЬКИХ КРАЇН І США ЩОДО ПРОТИДІЇ ЗЛОЧИННОСТІ У ФІНАНСОВІЙ СФЕРІ

В умовах ринкових перетворень, особливо в період загострення кризових явищ, привабливою для випробовування нових злочинних технологій є фінансова сфера. У ній протягом 2002−2009 рр. викрито понад 30 тис. злочинів (питома вага злочинів, учинених безпосередньо в банках, становить майже третину), а завдана шкода щорічно зростає (за підсумками 2009 р. – 40 % усіх втрат від економічної злочинності).

Збитки від злочинності у фінансовій сфері стають відчутними останнім часом, коли в країнах Європи та Північній Америці з'явились ряд гучних справ про шахрайство, які значно підірвали престиж ряду всесвітньо відомих компаній, шкода по яких перевищила валовий внутрішній продукт багатьох держав світу. Приміром, результатом шахрайських дій керівництва енергетичної компанії "Enron" наприкінці 2001 р. стали втрати службовців та акціонерів в розмірі кількох мільярдів доларів.

У західній доктрині вияви фінансової злочинності ототожнюється з поняттям "фінансове шахрайство". Фінансове шахрайство знаходить вияв всередині окремих держав та, водночас, охоплює території багатьох країн, набуває транснаціонального характеру. За оцінками міжнародних

експертів, прибутки фінансових шахраїв посіли друге місце після наркобізнесу. Скажімо, у США фінансові шахрайства вважають найнебезпечнішим різновидом "білокомірцевої" злочинності на кшталт виявам тероризму. Враховуючи зазначене, а також беручи до уваги, що ринкові відносини в Україні інтегрується до світового господарства, важливим є вивчення національних особливостей боротьби з шахрайством в інших країнах, відстежувати позитивні та негативні аспекти законодавчої та правозастосовної практики, а також засобів протидії у рамках міжнародної співпраці.

Більшість фінансових правопорушень у законодавстві європейських держав визнаються злочинами під впливом актів міжнародного права. Зокрема, Конвенцією про захист фінансових інтересів Європейських співтовариств (1995 р.) для імплементації у національне законодавство запропоновано перелік "злочинних шахрайських дій як невигідних для інтересів ЄС". Завдяки рекомендаціям ЄС склади злочинів проти фінансової системи у кримінальних кодексах багатьох європейських країн ретельно систематизовано (гл. 21 "Винні діяння у сфері економіки" КК Естонії; гл. 7 "Злочини проти фінансової системи" КК Болгарії тощо). Аналогічним чином структуровані ці злочинні діяння у кодексах Литви, Польщі, Швейцарії, Франції, Іспанії, Бельгії.

В основі усіх злочинів фінансового спрямування за КК ФРН є фінансовий обман, різновидами якого визнають: комп'ютерне шахрайство, одержання субсидій шляхом шахрайства, шахрайство у сфері кредитування. Прийнята у КК Нідерландів дефініція шахрайства є ширшою, ніж застосована у КК України. До фінансового шахрайства відносять дії, починаючи від обману страховиків до зловживань у сфері державних закупівель. Фінансовим шахрайством, згідно КК Франції, визнаються дії, спрямовані на те, щоб під час публічних торгів за допомогою подарунків, обіцянок, змови або внаслідок застосування будь-якого іншого шахрайського способу усунути особу, яка набавляє ціну, або обмежити надбавку ціни чи кількість замовлень. Законодавство Австрії значну увагу приділяє захистові вкладників та інвесторів від шахрайських посягань. Зокрема, "фінансовою пірамідою" визнається "система очікування прибутку, учасникам якої надається можливість отримати майнову винагороду за умови, що до цієї чи залежної від неї системи залучаються інші учасники на тих самих умовах, і за якої отримання майнової вигоди залежить від пов'язаного з умовами поведінки кожного наступного учасника".

Особливий інтерес мають норми законодавства та практика його застосування правоохоронними органами США. Ця країна набагато раніше інших зустрілась з різними видами фінансового шахрайства та

напрацювала значний досвід протидії. У переліку "білокомірцевих" злочинів, що складається з 50 рядків, категорія "фінансове шахрайство" стосується майже 60 % позицій. Фінансове шахрайство за законодавством США поділяється на такі види: "звичайний шахрайський обман" – навмисне перекручення фактів або використання прийомів, що уводять в оману, щоб отримати кошти чи майно; шахрайство з кредитними картами – використання платіжної карти чи банкомата у шахрайських цілях; "крадіжка особи" – використання статусу іншої особи або незаконне привласнення чужої посади з метою одержання незаконних прибутків; шахрайство, пов'язане з банкрутством – приховування активів, неправдиві заяви, введення в оману кредиторів тощо; шахрайство у сфері страхування – шахрайські дії, вчинені страховиками, страхувальниками чи особами, які надають певні страхові послуги; комп'ютерне шахрайство – незаконне використання комп'ютера або інших електронних засобів комунікації; шахрайство проти урядових установ – це шахрайство, вчинене у зв'язку із укладенням контрактів з урядом США та реалізацією федеральних програм, включаючи шахрайство у сфері будівництва житла; шахрайство у сфері обігу цінних паперів – передбачає їх викрадення шляхом маніпуляцій на ринку, шляхом використання електронних мереж і систем; ухилення від сплати податків – це шахрайство, вчинене шляхом подання неправдивих податкових звітів.

Підрозділи, створені для розслідування фінансових злочинів, як правило, називають "групами фінансових розслідувань". Термін "фінансові розслідування" застосовується міжнародними організаціями, створеними для боротьби з відмиванням коштів, зокрема Групою з розробки фінансових заходів боротьби з відмиванням грошей (FATF), Робочою групою країн Карибського басейну щодо здійснення фінансових заходів проти відмивання коштів тощо.

Спеціальні підрозділи відповідного профілю створені у країнах пострадянського простору. Приміром, питаннями податкових і фінансових злочинів в Республіці Білорусь займається Департамент фінансових розслідувань Комітету державного контролю, у Росії – Федеральна служба з фінансового моніторингу, у Молдові – Центр по боротьбі з економічною злочинами та корупцією.

Недосконала банківська діяльність може спричинити хаос на фінансовому ринку та економічний крах. Світова фінансова криза показала, що банківські структури, діяльність яких не прозора, або базується на особливих відносинах (наприклад, з якоюсь однією галуззю промисловості, родинних чи дружніх), або такі, що не мають чіткої кредитної політики, в умовах послабленого контролю за їх діяльністю з боку центрального банку, неминуче завдадуть шкоди нормальному розвитку

фінансового ринку. Більше того, криза банківського сектору, який є національним механізмом проведення платежів та відіграє ключову роль у всій економіці, може мати більш серйозний вплив на систему порівняно з кризовими ситуаціями у сфері небанківських фінансових посередників.

За своєю суттю банківська діяльність є ризикованою, тому більшість країн світу формує системи гарантування фінансової безпеки. Їх основною метою є забезпечення стійкості фінансової системи країни та її захист від зовнішніх і внутрішніх криз. Пріоритетним напрямом у питаннях запобігання використанню банків з протиправною метою є недопущення потрапляння до банківської системи коштів, одержаних злочинним шляхом. Саме з цією метою, а також в межах дій по імплементації нової редакції Сорока рекомендацій FATF, затвердженої Берлінським засіданням групи в червні 2003 року, необхідно законодавчо передбачити наступне:

- заборонити банкам встановлювати кореспондентські відносини з банками, іншими фінансовими установами-нерезидентами, що не мають постійного місцезнаходження та не здійснюють банківської діяльності за місцем своєї реєстрації, або не підлягають нагляду в країні свого перебування, а також банками, іншими фінансовими установами, які підтримують такі кореспондентські відносини;
- можливість отримання Національним банком інформації від державних органів, необхідної для визначення ділової репутації та фінансового стану осіб, які претендують на зайняття посад керівників банків або мають намір придбати істотну участь у банку;
- заборону залучення до капіталу банку коштів з непідтверджених джерел.

Для забезпечення виконання банками важливої ролі у розвитку фінансового ринку – як кредиторів, або кредитних посередників та агентів контролю за використанням коштів, необхідною умовою є розроблення та впровадження системи ефективних норм, які забезпечували б безпеку та стабільність фінансової системи.

У цілому ж, на нашу думку, в Україні вдалося створити систему норм, яка здатна належним чином протидіяти злочинам у фінансовій сфері, проте національному законодавцю іноді бракує прагматичності, виваженості та послідовності в рішеннях, вміння максимально точно і швидко передбачати негативні тенденції у фінансовій системі держави. На жаль, нові види та форми злочинної діяльності далеко не завжди фіксуються в кримінальному законодавстві, що часом змушує міжнародне чи європейське співтовариство запроваджувати відповідні санкції проти нашої держави. Тому вважаємо, що Україні в майбутньому слід

активізувати зусилля щодо додержання міжнародних та європейських стандартів з приводу протидії злочинам у фінансовій сфері, а також ефективно використовувати позитивний іноземний досвід цього питання. Цього вимагають стан системи господарювання, глобалізація економічних зв'язків, процеси євроатлантичної інтеграції.

В.В. Корольчук, *канд. юрид. наук,*
науковий співробітник відділу з організації науково-дослідної роботи
Національної академії внутрішніх справ

ЗАПОБІГАННЯ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЮ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ, У БАНКАХ

Здійснення внутрішнього контролю з метою протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, включають в себе програми:

а) ідентифікації і вивчення Банком своїх клієнтів;
б) виявлення в діяльності клієнтів операцій, що підлягають обов'язковому контролю, і інших операцій з грошовими коштами або майном, пов'язаних з легалізацією (відмиванням) доходів, одержаних злочинним шляхом;
в) документального фіксування інформації про ідентифікацію клієнтів;
г) зберігання інформації і документів, одержаних внаслідок реалізації програм здійснення внутрішнього контролю;
д) навчання працівників Банку питанням протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом;
е) організації в Банку роботи по протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом.

Основним і самим ефективним методом боротьби з відмиванням доходів, одержаних злочинним шляхом, на рівні Банку є ідентифікація клієнта і вивчення його діяльності (фінансових операцій).

Критерії віднесення клієнта Банку до осіб з високим ризиком здійснення легалізації (відмивання) доходів, одержаних злочинним шляхом:

По географічній ознаці:

1. Клієнти, зареєстровані в державах (територіях), про які з міжнародних джерел відомо, що вони не дотримують загальноприйнятих стандартів в боротьбі з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або є державами (територіями) з підвищеним рівнем злочинності і корупції.
2. Клієнти, зареєстровані в державах (територіях), де не передбачене розкриття або представлення інформації при проведенні фінансових операцій.

3. Клієнти не виконують рекомендацій Групи розробки фінансових заходів боротьби з відмивання грошей (FATF).
4. Клієнтами є держави, в яких відбуваються військові дії.

По видах діяльності:

1. Діяльність юридичних осіб (їх відособлених підрозділів), що не є кредитними організаціями, що займаються переказами платежів в готівковій формі по чеках, інкасацією грошових коштів, обміном валют на основі агентських угод.
2. Діяльність юридичних осіб, зареєстрованих в офшорних зонах, їх відособлених підрозділів, дочірніх і залежних від них підприємств.
3. Гральний бізнес (підприємницька діяльність, що не є реалізацією продукції (товарів, робіт, послуг), пов'язана з витяганням гральним закладом прибутків від участі в азартній грі і парі прибутку у вигляді виграшу і плати за їх проведення).
4. Торгівля (особливо експорт) зброєю і її компонентами.
5. Операції з цінними паперами з використанням готівкових коштів, послуги по отриманню ПДВ.
6. Заняття туристичною діяльністю.
7. Здійснення зовнішньоекономічних операцій.
8. Юридична особа є добродійною громадською організацією (крім організацій, діючих під егідою відомих міжнародних організацій).
9. Юридична особа, яка отримує фінансову допомогу від нерезидента або що надає фінансову допомогу нерезиденту.
10. Клієнт займає (займав) посаду і має (мав) владні повноваження (керівний склад центральних і місцевих органів державної виконавчої влади, місцевого самоврядування, осередків політичних партій) або є членом сім'ї такої особи.

Ніякі з вище перерахованих видів діяльності не є заздалегідь сумнівними, але клієнти, що здійснюють їх, повинні бути на особливому контролі підрозділів Банку.

Орієнтовний перелік критеріїв віднесення фінансових операцій до таких, що можуть підлягати внутрішньому фінансовому моніторингу (не є вичерпним).

Надання кредиту під забезпечення у вигляді гарантії нерезидента за умови відсутності очевидного зв'язку між місцем діяльності клієнта і його контрагентів і місцезнаходженням гаранта, особливо якщо гарантія видається філією нерезидента.

Погашення простроченої заборгованості за кредитним договором, якщо умови діяльності особи та інформація, якою володіє суб'єкт первинного фінансового моніторингу щодо цієї особи, не дають можливості встановити джерела походження коштів для погашення заборгованості.

Дострокове погашення кредитів коштами із не зазначених особою або невідомих для суб'єкта первинного фінансового моніторингу джерел погашення.

Проведення фінансових операцій по внесенню до статутних фондів господарських товариств цінних паперів у розмірах, що перевищують 50 % статутного фонду підприємства, що реєструється.

Купівля особами-резидентами за договорами доручення пакетів акцій (часто неліквідних) українських суб'єктів підприємницької діяльності у фірм-нерезидентів за цінами, значно вищими їх ринкової вартості.

Регулярне здійснення особою фінансових операцій з векселями, якщо дана особа не виступає емітентом або отримувачем коштів за цими векселями та не має ліцензії професійного учасника ринку цінних паперів.

Набуття прав власності на пакет цінних паперів, сумарна номінальна вартість яких дорівнює або перевищує 80 000 грн. чи є еквівалентною цій сумі в іноземній валюті, за договорами дарування або міни.

Купівля-продаж, без участі торговця цінними паперами, пакета цінних паперів, вартість якого дорівнює чи перевищує 80 000 грн.

Регулярні операції з купівлі з подальшим продажем цінних паперів, що не мають котирування і не обертаються вільно на організованому ринку цінних паперів, за умови, що прибуток від реалізації цінних паперів спрямований на придбання високоліквідних цінних паперів, що вільно обертаються на організованому ринку.

Одночасне виставляння клієнтом доручень на купівлю і продаж цінних паперів й інших фінансових інструментів за цінами, що мають помітне відхилення від поточних ринкових цін за аналогічними угодами.

Отримання грошових коштів з рахунку, відкритого у фінансовій установі в країні, що віднесена Кабінетом Міністрів України до переліку офшорних зон.

Сплата резидентом нерезиденту неустойки (пені, штрафу) за невиконання договору поставки товарів (виконання робіт, надання послуг) або за порушення умов договору, якщо розмір неустойки перевищує 10 % від суми непоставлених товарів (невиконаних робіт, ненаданих послуг).

Неможливість визначення предмету зовнішньоекономічних операцій. Відсутність чіткого опису товарів, робіт, послуг, що є предметом зовнішньоекономічного договору/контракту.

Придбання особою іноземної валюти для погашення кредиту, отриманого того ж або попереднього банківського дня під зовнішньоекономічний контракт іншою особою або на підставі договору поручительства.

Регулярне повернення платникам коштів, відправлених за кордон.

Регулярне розірвання договорів страхування (повернення страхових платежів).

Регулярне повернення страхових платежів на рахунок клієнта за договорами страхування при помилковому або надлишковому перерахуванні.

Регулярна купівля/продаж товарів на суму, що дорівнює або перевищує 80 000 грн. чи є еквівалентною цій сумі в іноземній валюті, за умови, що платежі здійснюються готівкою.

Купівля в ігровому закладі ігрових фішок на суму, що дорівнює або перевищує 10 000 грн. чи є еквівалентною цій сумі в іноземній валюті.

Регулярне та циклічне здійснення фінансових операцій з купівліпродажу активів без фактичної поставки активів між учасниками операції.

Клієнтом виступає особа, яка обіймає (обіймала) посаду, відповідно до якої має (мала) широкі владні повноваження (керівний склад центральних і місцевих органів державної виконавчої влади, місцевого самоврядування, осередків політичних партій), або є членом сім'ї такої особи.

Якщо клієнт здійснює операції з цінними паперами на пред'явника з одним контрагентом і вказує це в платіжному дорученні і операція підпадає під ознаки обов'язкового моніторингу (Код 5010), при цьому він здійснює перерахування не єдиним платежем, а вважає за доцільне дробити загальну суму то в такому випадку моніторинг цих операцій здійснюється наступним чином:

- якщо клієнт під час дроблення не уникає обов'язкового моніторингу (Код 5010) то всі платежі на суму менше 80 000,0 грн. не підпадають під ознаку внутрішнього моніторингу (Код 300);
- в різі здійснення клієнтом дроблення всіх платежів на суму менше 80 000,0 грн., якщо загальна сума таких платежів дорівнює 80 000,0 грн. і більше то всі ці операції підпадають під ознаку внутрішнього моніторингу (Код 300).

В разі здійснення фізичною особою операцій (купівлі/продажу) з великого пакету цінних паперів, що вільно не обертаються на організованому ринку, за умови, що особа не є професійним учасником ринку цінних паперів і цінні папери не передаються особі в погашення простроченої заборгованості контрагента перед особою, всі ці операції підпадають під ознаку внутрішнього моніторингу (Код 900).

Література

1. Закон України “Про банки і банківську діяльність”.
2. Закон України “Про запобігання і протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом” від 28.11.2002 року (зі всіма змінами і доповненнями).
3. Закон України “Про фінансові послуги і державне регулювання ринків фінансових послуг”.
4. Постанова Кабінету Міністрів України і Національного Банку України “Про сорок рекомендацій Групи з розробки фінансових заходів щодо боротьби з відмиванням грошей (FATF)” від 08.08.01 № 1124.
5. Постанова Кабінету Міністрів України і Національного Банку України “Про затвердження плану заходів на 2008 рік із запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансування тероризму” від 19 березня 2008 р. № 228.
6. Постанова Національного Банку України “Про порядок накладення Національним банком України штрафів за порушення банками вимог Закону України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом від 17.03.04 № 108.
7. Постанова Правління Національного банку України “Про затвердження Положення про здійснення банками фінансового моніторингу” від 14.05.2003 року № 189 (зі всіма змінами і доповненнями).
8. Постанова Правління Національного банку України “Про затвердження Інструкції про порядок відкриття, використання і закриття рахунків у національній та іноземних валютах” від 12.11.2003 року № 492.
9. Постанова Правління Національного банку України “Про затвердження Інструкції про безготівкові розрахунки в Україні в національній валюті” від 21.01.2004 року № 22 (зі всіма змінами і доповненнями).
10. Постанова Правління Національного банку України “Про затвердження Правил здійснення переказів іноземної валюти за дорученням та на користь фізичних осіб” від 29.12.2007 року № 496;
11. Рішення Державної комісії з цінних паперів та фондового ринку “Про затвердження Положення про здійснення фінансового моніторингу учасниками ринку цінних паперів” від 4 жовтня 2005 року № 538.

Ю.О. Левченко, *канд. юрид. наук,*
доц. кафедри кримінології та кримінально-виконавчого права
Національної академії внутрішніх справ

ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЮ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ, У СФЕРІ ПАЛИВНО-ЕНЕРГЕТИЧНОГО КОМПЛЕКСУ

Захист об’єктів паливно-енергетичного комплексу (далі – ПЕК) від злочинних посягань є одним з пріоритетних напрямів діяльності правоохоронних органів, тому що підприємства ПЕК виробляють не менше 5 % національного доходу і забезпечують більше 25 % валютних надходжень.

Розслідування злочинів, що вчиняються у сфері ПЕК, викликає труднощі в значній мірі із-за різноманіття цих злочинів, а також їх специфічність, що вимагає від слідчого знань в області ведення обліку та особливостей самого виробництва, характерних для цієї області. Найчастіше для виявлення, розкриття і подальшого успішного розслідування потрібні спільні зусилля не лише оперативно-розшукових і слідчих підрозділів, але й використання ресурсів і можливостей зацікавлених у запобіганні з такими злочинами організацій паливно-енергетичного комплексу, наприклад їх охоронних структур, здатних, наприклад, самостійно виявити незаконні "врізання" в трубопроводи. Нерідко приводом для порушення кримінальної справи є саме заява про злочин, яка надійшла до органів внутрішніх справ від організацій-власників, які постраждали від вчинених злочинів.

Аналіз кримінальних справ і матеріалів дозволив виділити наступні основні способи вчинення злочинів у сфері переробки нафти і поставок нафтопродуктів.

1. Незаконна переробка нафти на "міні-заводів". "Міні-заводи", як правило, називають незаконні кустарні заводи або "підпільні" цеха, створені для незаконного виготовлення пального і пально-мастильних матеріалів шляхом переробки сирої нафти. Зазвичай до них постачається нафта, незаконно добута або викрадена (за допомогою "врізок" з магістральних нафтопроводів, шахрайства або присвоєння), яка переробляється з використанням саморобних перегінних установок. З огляду на низьку потужність саморобних установок, переробка нафти, паркан якої здійснюється з декількох врізок в нафтопровід, здійснюється звичайно на декількох міні-установках. Відповідно, отриманий бензин, моторні масла володіють низькою якістю, проте успішно реалізуються на всій території України. Даний вид злочинної діяльності пов'язаний з ухиленням від державної реєстрації та контролю (отримання ліцензій, дотримання їх умов, порушення податкової і касової дисципліни тощо.)

2. Розкрадання нафтопродуктів з використанням службового становища. Використання службового становища значно підвищує ступінь суспільної небезпеки вчинених злочинів. Особи, які виконують управлінські функції, мають професійними знаннями і досвідом, добре знають не тільки технологію виробництва, але і особливості обліку та контролю руху матеріальних цінностей, мають широке коло соціальних і злочинних зв'язків, що дозволяє ретельно спланувати вчинення злочину, підібрати необхідних для участі осіб, розробити витончені способи злочинів, послабити систему господарсько-фінансового контролю, що діє на підприємстві, приховати сліди злочинів тощо. Це ж створює додаткові труднощі при розкритті та розслідуванні таких злочинів.

3. Контрабанда нафтопродуктів, учинена в обхід митних постів характерна для прикордонних областей України. Одним з факторів, що сприяють значну поширеність даного способу вчинення злочинів, є не облаштованість державного кордону з республіками колишнього Радянського Союзу. При ввезенні нафтопродуктів із за кордону морським транспортом використовується інший спосіб обходу митного контролю – під виглядом бункерування. При бункеруванні спеціальними "суднами-бункеровщика" здійснюється перевантаження нафтопродуктів (дизпаливо, топковий мазут, бензин) з берегових нафтобаз через нафто райони порту на іноземні судна. Проте для організацій – перегрузчіков (зокрема, порту) не має значення, в яких цілях будуть використовуватися перевантажуються, нафтопродукти.

4. Ухилення від сплати податків. Підприємства, що здійснюють переробку нафти та поставки нафтопродуктів, використовують самі різні схеми ухилення від сплати податків. Наприклад, здійснення фірмами бартерних і взаємозалікових операцій, які не обкладаються податком. Існує і ряд інших способів ухилення від сплати податків, у тому числі такі, як неправомірне збільшення витрат на переробку нафтопродуктів, набуття у залік поставлених нафтопродуктів цінних паперів, заниження обсягів поставок нафтопродуктів, перерахування грошових коштів на рахунки третіх, часто спеціально створених для цих цілей "підставних" фірм, розрахунок неврахованими готівковими коштами, спеціальне заплутування або відсутність бухгалтерського обліку.

5. Крадіжка, вчинена за допомогою пристрою "відводів" від сховищ нафтопродуктів і трубопроводів – приєднання до сховища або трубопроводу додаткової несанкціонованої магістралі для вчинення кількаразових розкрадань. Таким способом вчиняють розкрадання нафтопродуктів особи, які мають на меті вчинювати систематичні крадіжки, для чого вони використовують більш складні, порівнюючи з "врізаннями", технічні пристрої та спеціальні ємності для накопичення нафтопродуктів. Цей спосіб є одним із різновидів "урізання", однак його головна відмінність полягає у тому, що при "врізанні" нафтопродукти безпосередньо викрадаються з трубопроводу, а при "відводі" накопичуються в ємності і за сприятливих умов вивозяться викрадачами.

6. Крадіжка, вчинена шляхом переливу нафтопродуктів у підготовлені заздалегідь ємності (проста крадіжка з елементом підготовки). Готуючись вчинити злочин цим способом, викрадачі, зазвичай, проводять розвідку. Встановлюють місця локалізації цистерн із нафтопродуктами на залізничній станції; з'ясовують розташування відбірних кранів; розшукують несанкціоновані "врізання", зроблені іншими особами;

виявляють місця стоянки транспорту, який перевозить нафтопродукти, тощо. Обов'язково готують ємності та шланги для зливу, а також інструменти (гайкові та газові ключі).

7. Крадіжки ємностей, у яких зберігаються нафтопродукти (автоцистерни, залізнична цистерна, бочка або інша тара), як правило, вчиняються групою злочинців з урахуванням обстановки та умов транспортування.

Готування до злочину у цьому разі полягає в попередньому з'ясуванні місць складування та зберігання тари з нафтопродуктами; отримання інформації про склад вантажних поїздів; установлення злочинцями графіків і маршрутів руху та стоянок автомобілів, що перевозять нафтопродукти. Крім того, готуючись вчинити крадіжку, викрадачі найчастіше спеціально виводять із ладу транспортні засоби, що перевозять продукцію, і надалі, відвертаючи увагу водіїв, викрадають ємності.

8. Крадіжки нафти (нафтопродуктів) з місць їх скупчення вчиняють при заповненні різних ємностей, коли такі продукти накопичуються у природних і штучних свердловинах і сховищах. Так, при аваріях, пов'язаних із пошкодженням магістрального трубопроводу, нафтопродукти, що розлилися, накопичують у природних заглибленнях рельєфу місцевості, а потім розкрадають. Під час наливання продукції на вантажних терміналах нафтопродукти, що пролилися, також накопичуються у природних і штучних заглибленнях, звідки їх розкрадають.

9. Крадіжка, вчинена за допомогою насосного устаткування, тобто відкачування нафти (нафтопродуктів) зі сховищ, ємностей, трубопроводів. Цей спосіб відрізняється від переливання нафтопродуктів у заздалегідь підготовлені ємності тим, що при ньому використовуються додаткові технічні засоби, за допомогою яких здійснюється механічне перекачування продукту, а не вільний перелив або "самоплив", що дозволяє вчинити розкрадання у більших обсягах з ємностей, доступ до яких іншим способом неможливий або надто ускладнений, наприклад, розкрадання з підземного сховища (на заправній станції, нафтобазі, нафтосховищі) або з танкерів нафтоналивного судна.

Вищенаведений перелік способів учинення крадіжок нафтопродуктів не є вичерпним, тому що з удосконалюванням технології переробки, зберігання і транспортування нафти й нафтогазопродуктів можна припустити вчинення крадіжок іншими способами. Таким чином, варто звернути увагу на узагальнення характеристик кожного з механізмів учинення крадіжок нафтогазопродуктів.

І.С. Пеліван, *здобувач кафедри кримінального процесу*
Київського національного університету внутрішніх справ

ПРИТЯГНЕННЯ ОСОБИ ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ВІДМИВАННЯ КОШТІВ БЕЗ ОБВИНУВАЧЕННЯ В ПРЕДИКАТНОМУ ЗЛОЧИНІ

Для встановлення можливості притягнення особи до відповідальності за ст. 209 КК України без попереднього або одночасного обвинувачення в предикатному злочині слід проаналізувати положення кримінального права щодо доказування злочинного походження предмета легалізації (відмивання) коштів. У науці кримінального права юристами висловлюються різні думки стосовно встановлення злочинного характеру походження предмета легалізації вироком суду. Скажімо, російські юристи (П. Г. Пономарьов, Д. І. Лескаєв, Л. К. Виноградова та ін.) вважають, що факт злочину, унаслідок якого одержано кошти та майно, для притягнення особи до відповідальності за їх відмивання має бути встановлено обвинувальним вироком суду.

Дещо іншу позицію зайняв Пленум Верховного Суду України, зокрема у п. 11 постанови "Про практику застосування судами законодавства про кримінальну відповідальність за легалізацію (відмивання) доходів, одержаних злочинним шляхом" від 15 квітня 2005 р. № 5, де зазначено, що притягнення особи до кримінальної відповідальності за ст. 209 КК можливе як за умови, що факт одержання нею коштів або іншого майна внаслідок вчинення предикатного діяння встановлено судом, так і в разі, коли вона не притягувалася до кримінальної відповідальності за предикатне діяння.

В останньому випадку особа одночасно притягується до кримінальної відповідальності за предикатний злочин та за легалізацію (відмивання) коштів або іншого майна, одержаних унаслідок його вчинення, тобто за сукупністю цих злочинів, оскільки вона усвідомлює, що вчиняє легалізацію таких коштів (майна).

Водночас вітчизняні дослідники (О.О. Дудоров, М.В. Бондарева, А.С. Беніцький), вважають, що обвинувальний вирок суду за цих обставин не потрібний. Прихильники тієї позиції, що цей вирок потрібен, апелюють до принципу презумпції невинуватості, відповідно до якого особа не може бути визнана винною у вчиненні злочину, доки її вину не буде доведено вироком суду. Між тим, як вірно зазначає О.О. Дудоров, реалізації цього принципу не суперечить та обставина, що у низці кримінально-правових норм йдеться про вчинення злочину особою

незалежно від того, чи встановлено це вироком суду [1]. Якщо уявити, що обвинувальний вирок суду потрібен у будь-якому випадку, то його винесення мало б передувати застосуванню, скажімо, ст. 38 КК (затримання особи, що вчинила злочин), ст. 44–48 КК (звільнення від кримінальної відповідальності особи, що вчинила злочин), ст. 198 КК (придбання або збут майна, завідомо здобутого злочинним шляхом), ст. 396 КК (приховування злочину) та ін.

З іншого боку, на практиці нерідко трапляються ситуації, коли особу, яка вчинила предикатний злочин, за певних умов, не може бути притягнуто до кримінальної відповідальності (переховується від слідства, померла, стала недієздатною тощо), а одержані нею кошти легалізуються іншими особами. До того ж, аналогічну ситуацію підтверджує практика застосування ст. 198 КК України, де достатньо лише усвідомлення особою злочинного характеру походження майна, при чому точна обізнаність про характер і конкретні обставини вчиненого предикатного злочину не є обов'язковою [2].

У ст. 209 і 198 КК України кримінальна відповідальність пов'язана з предметом, одержаним злочинним шляхом. Схожість цього формулювання, може, на нашу думку, бути одним з аргументів того, що для кваліфікації відмивання грошей не треба встановлювати факт предикатного злочину обвинувальним вироком суду. Крім того, встановлення факту предикатного злочину обвинувальним вироком суду буде означати, що цей злочин фактично розкрито, а кошти, здобуті унаслідок вчинення предикатного злочину підпадають під ознаки "спеціальної конфіскації", передбаченої кримінально-процесуальним законодавством. Утім це не логічно, оскільки ст. 209 КК передбачає окрему відповідальність саме за використання майна, здобутого злочинним шляхом. Це майно є предметом легалізації, і бути, водночас, конфіскованим за вчинення предикатного злочину, не може.

Обґрунтування можливості притягнення особи до відповідальності за ст. 209 КК України без засудження її за вчинення предикатного злочину підтверджує і зарубіжна практика.

Наприклад, для притягнення особи до кримінальної відповідальності за відмивання грошей за законодавством США вердикт судового органа про предикатний злочин не є обов'язковим. Яскравим свідченням тому є добре всім відома справа з обвинувачення у відмиванні коштів Павла Лазаренка. Районним судом Північної Каліфорнії він був визнаний винним у "змові з метою відмивання грошей (ст. 18 Федерального Кодексу США, § 1956 (h)); відмиванні грошей (ст. 18 Федерального Кодексу США, § 1956 (a)(2)); перевезенні викрадених цінностей

(ст. 18 Федерального Кодексу США, § 2314)". За даними розслідування, П. Лазаренко протягом 1994–1997 рр. займався на території України протизаконною діяльністю, унаслідок чого дістав матеріальні цінності. Установлено, що Лазаренко вчинив: викрадення майна шляхом незаконного привласнення й обману на порушення ст. 18 Федерального Кодексу США, § 2314 та 2315; вимагання, визначене ст. 18 Федерального Кодексу США, § 1956 (c) (7) (B) (ii) та шахрайство на порушення ст. 18 Федерального Кодексу США, § 1343 [3]. Отже, для американської сторони необов'язковою була наявність вироку суду про визнання Лазаренка винним у вчиненні злочинів на території України.

Наявність обвинувального вироку суду щодо особи, яка вчинила "предикатний" злочин, не є обов'язковою умовою її притягнення до кримінальної відповідальності за відмивання коштів і за законодавством ФРН та низки інших європейських країн.

Цю позицію слід визнати правильною. Доказом факту злочинного походження майна може бути не лише обвинувальний вирок суду, а й будь-які об'єктивні дані щодо особи, яка здобула доходи. Про цю обставину йдеться у п. "c" § 2 ст. 6 Страсбурзької конвенції 1990 р. "Про відмивання, виявлення, вилучення та конфіскацію доходів від злочинної діяльності", згідно якої "усвідомлення, намір і мета як необхідні складові елементи одного з правопорушень, зазначених у цьому пункті, можуть бути встановлені виходячи з об'єктивних, фактичних обставин справи".

Тобто очевидним стає висновок, що притягнення особи до відповідальності за ст. 209 КК можливе за таких альтернативних умов:

1) злочинність предикатного діяння встановлено судом у відповідних процесуальних документах (обвинувальному вироку, постановах чи ухвалах про звільнення від кримінальної відповідальності, про закриття справи з нереабілітуючих підстав тощо);
2) особа одночасно притягується до кримінальної відповідальності за предикатний злочин і за легалізацію (відмивання) доходів, одержаних унаслідок його вчинення;
3) особу притягують до кримінальної відповідальності за легалізацію (відмивання) доходів, одержаних злочинним шляхом, за умов усвідомлення нею ознак предикатного злочину, та доведення цього факту матеріалами кримінальної справи.

Література

1. Дудоров О.О. Злочини у сфері господарської діяльності: кримінально-правова характеристика. – К.: Юридична практика, 2003. – С. 517.
2. Коржанский М. И. Ответственность за приобретение, хранение и сбыт имущества, добытого преступным путем / М. И. Коржанский : учеб. пособие. – Волгоград, 1971. – С. 34.
3. Обвинувальний висновок у справі П. Лазаренка // Іменем закону. – 2000. – № 26. – С. 8–9.

О.М. Ващенко, *аспірант*
ДВНЗ "Українська академія банківської справи Національного банку України", м. Суми

СИНЕРГЕТИЧНИЙ ЕФЕКТ У РОБОТІ СИСТЕМИ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ НЕЗАКОННИХ ДОХОДІВ У БАНКІВСЬКІЙ СИСТЕМІ

Елементом фінансової і економічної системи країни, без участі якого легалізація доходів, отриманих злочинним шляхом та фінансування тероризму неможливі, є банківська система країни, що виступає не лише як посередник між учасниками легалізації незаконних доходів, але й як самостійний учасник процесу легалізації. За даними Державного комітету фінансового моніторингу України найбільш активним суб'єктом первинного фінансового моніторингу є банківські установи, які надсилають близько 97 % повідомлень про операції, що підлягають фінансовому моніторингу. Так протягом 2009 року Держфінмоніторингом було отримано 896 508 повідомлень про операції, що підлягають фінансовому моніторингу. З них від банківських установ було отримано 868 357. Тому найбільший ефект для протидії легалізації доходів отриманих злочинним шляхом дадуть саме заходи в банківській сфері.

Головною проблемою системи протидії легалізації незаконних доходів в банківській системі України є відсутність синергетичного ефекту та взаємодії між окремими положеннями законодавства, що призводить до фактичної непрацездатності. Маємо типовий приклад формального підходу, коли всі дії були спрямовані не на побудову реально працюючої системи саме в умовах України, а на задоволення вимог міжнародних організацій та на відповідність стандартам розвинених країн. Свідченням непрацездатності діючої системи є наднизький коефіцієнт її корисної дії (ККД). Якщо в якості такого коефіцієнту обрати співвідношення справ, що дійшли до суду (правильніше, мабуть, було б розглядати кількість справ, за якими було винесено вирок, але в такому випадку ККД дорівнював би 0) до кількості повідомлень, то за 2009 рік ККД системи протидії легалізації доходів, отриманих злочинним шляхом і фінансуванню тероризму дорівнював 0.0167. Тобто система не

працює і вимагає суттєвих удосконалень. Оскільки близько 97 % повідомлень надходить до Держфінмоніторингу від банківської системи, саме в цій сфері слід робити удосконалення.

Головною проблемою є те, що одні положення нормативних актів не взаємодіють з іншими. Наприклад, банки зобов'язані здійснювати ідентифікацію клієнтів та проводити політику "знай свого клієнта". Це міжнародна практика, яка допомагає вже на початкових стадіях уникнути проблем з легалізацією незаконних доходів в банку. Згідно з іншими положеннями, банки зобов'язані повідомляти Уповноважений орган про всі операції, сума яких перевищує певний ліміт (на теперішній час це 150 000 грн.). Дана сума є адекватною і корелює з розмірами операцій, що підлягають фінансовому моніторингу в інших країнах. Але операцій на такі суми особливо в системних банках бувають сотні в день. Відповідно кожну треба обробити, направити до Уповноваженого органу. Це досить значний обсяг роботи, яка на 90 % є непотрібною, оскільки основна маса операцій проводилась клієнтами, що не мають жодного відношення до відмивання "брудних" грошей чи фінансування тероризму. Банк про це знає, оскільки проводить політику "знай свого клієнта", але за законом має доводити всю інформацію до Уповноваженого органу. В результаті збільшуються обсяги роботи і Уповноваженого органу, який замість того, щоб більше ретельно розглядати дійсно підозрілі операції, аналізує завідомо законні фінансові потоки. В результаті ефективність системи і без того низька не може не падати.

Виходом з цієї ситуації є забезпечення взаємодії між окремими складовими законодавства і досягнення синергетичного ефекту від його роботи.

Окреслимо базові підходи для цього. Першим кроком має бути поєднання ідентифікації клієнта та політики "знай свого клієнта" з моніторингом транзакцій та звітністю до Уповноваженого органу.

Не потрібно повідомляти Уповноважений орган та здійснювати моніторинг всіх фінансових операцій. Якщо фінансова операція здійснюється клієнтом, який в банку не викликає сумнівів на предмет потенційної участі у легалізації незаконних доходів чи фінансуванню тероризму, вона не має підлягати фінансовому моніторингу. І, навпаки, якщо клієнт та його операції викликають підозру у банку, обов'язковому моніторингу можуть піддаватись навіть операції, що формально є законними, тобто не перевищують суму в 150 000 грн, таким чином можна буде паралельно боротись із структуруванням.

Необхідно на законодавчому рівні розробити і закріпити методику, щодо визначення рівня довіри клієнта та дій банку в сфері фінансового моніторингу, залежно від нього (рівня довіри).

Для визначення рівня довіри доцільно використовувати бінарну методику експрес-оцінки на базі ряду критеріїв, підсумок балів за всіма критеріями дозволить визначити рівень довіри до клієнта. Перелік пропонованих критеріїв та їх бінарна оцінка наведені в таблиці 1.

Таблиця 1

Критерії для визначення рівня довіри клієнта та їх бінарні оцінки

№	Критерій	Бінарна оцінка у випадку відповідності	
		Так	Ні
1	В історії клієнта не було випадків операцій, що були класифіковані як легалізація злочинних доходів або фінансування тероризму	1	0
2	Серед власників істотної участі в статутному фонді клієнта немає осіб, що були пов'язані з легалізацією злочинних доходів або фінансуванням тероризму	1	0
3	Серед найбільших контрагентів клієнта немає таких, що були пов'язані з легалізацією злочинних доходів або фінансуванням тероризму	1	0
4	Серед контрагентів клієнта немає офшорних компанії	1	0
5	Серед власників істотної участі в статутному фонді клієнта немає осіб, що володіють офшорними компаніями	1	0
6	Серед власників істотної участі в статутному фонді найбільших контрагентів клієнта немає таких, що були пов'язані з легалізацією злочинних доходів або фінансуванням тероризму	1	0
7	Серед власників істотної участі в статутному фонді найбільших контрагентів клієнта немає таких, що володіють офшорними компаніями	1	0
8	Серед найбільших контрагентів клієнта немає таких, що часто здійснюють операції з/через офшорні компанії	1	0
9	Діяльність клієнта і походження коштів зрозумілі банку	1	0
10	Відповідно до критеріїв, визначених в Постанові НБУ № 189 клієнт банку є клієнтом з низьким рівнем	1	0

Пропонується розділити всіх клієнтів банку на п'ять категорій, залежно від рівня довіри до нього. Пропонований розподіл рівнів довіри за кількістю балів та рекомендовані дії з фінансового моніторингу банку наведені в таблиці 2.

Таблиця 2

Розподіл рівнів довіри за кількістю набраних балів і рекомендовані дії з фінансового моніторингу їх операцій

Рівень довіри до клієнта	Кількість балів	Фінансовий моніторинг операцій в банку
Абсолютний	9–10	Не здійснюється
Високий	7–8	Здійснюється у випадках значного перевищення суми операції законодавчо визначеної суми
Звичайний	5–6	Здійснюється у звичайному режимі (повідомляється Уповноважений орган у випадках перевищення суми по операції еквівалентну 150 000 грн)
Низький	3–4	Здійснюється посилений контроль за здійсненими операціями з обов'язковим повідомленням Уповноваженого органу, додатковий аналіз контрагентів за операцією
Відсутній	0–2	Операція зупиняється або кожна операція ретельно перевіряється та повідомляється про її здійснення Уповноважений орган

Банк згідно з запропонованою класифікацією, визначає рівень довіри до клієнта та здійснює дії з фінансового моніторингу відповідно визначеного рівня.

ПІДБИТТЯ ПІДСУМКІВ РОБОТИ КОНФЕРЕНЦІЇ!

Шановні колеги! За ініціативи Національного банку України, Міністерства внутрішніх справ України, Української академії банківської справи Національного банку України та Національної академії внутрішніх справ у Севастопольському інституті банківської справи УАБС НБУ проведена науково-практична конференція, присвячена питанням боротьби з економічними злочинами, які вчиняються з використанням комп'ютерних мереж.

Зважаючи на всі наявні проблеми та труднощі щодо розкриття теми безпеки та захисту бізнесу в Україні, стає актуальною потреба в знаннях, які надаються в рамках навчальних дисциплін цього спрямування.

У відповідних курсах дисциплін студенти та курсанти повинні вивчати теми, присвячені уразливостям та основним загрозам безпеці, видам шахрайства в електронному бізнесі та засобам запобігання їх, розглядати законодавчі акти, які визначають державне регулювання електронної комерції в Україні, а також межі відповідальності за порушення відповідного законодавства.

Одними з найважливіших умов поширеного застосування Інтернету в електронному бізнесі було й є забезпечення адекватного рівня безпеки для всіх транзакцій. Це стосується інформації, що передається між користувачами; зберігається в базах даних торговельних мереж; супроводжує фінансові операції.

Поняття безпеки ведення бізнесу в цілому та поняття безпеки інформації, що передається, можна визначити як стан стійкості інформації до випадкових і передбачених дій, що виключає ризики її знищення, викривлення та розкриття, які мають наслідки у вигляді матеріальної шкоди власника чи користувача інформації. Враховуючи те, що мережа цілком відкрита для зовнішнього доступу, роль цих методів дуже велика.

У межах навчальних курсів необхідно розглядати розділи, які освітлюють цю проблему. Насамперед – це поняття криптографії – науки про забезпечення безпеки даних. Криптографія вирішує завдання конфіденційності, аутентифікації та цілісності інформації. Згідно з вказаними завданнями основними методами забезпечення безпеки є шифрування, цифровий підпис, сертифікати. До найбільш поширених механізмів, які повинні вирішити визначені завдання та забезпечити безпеку проведення електронних платежів через Інтернет, сьогодні можна віднести такі:

- протокол SSL (Secure Socket Layer), що забезпечує шифрування даних, які передаються через Інтернет;
- стандарт SET (Secure Electronic Transactions), розроблений компаніями Visa та MasterCard, забезпечує безпеку та конфіденційність укладання договорів за допомогою пластикових карток.

Треба також підкреслити необхідність подальшого аналізу суспільної небезпеки, яку являють собою прояви кіберзлочинності в банківській сфері, а також виявлення криміногенних чинників, що породжують або обумовлюють вчинення відповідних видів злочинів, розробки і подальшого впровадження послідовних заходів щодо їх попередження і протидії.

Науково-практичний форум повинен всебічно і комплексно підкреслити актуальні проблеми, які належать до безпеки діяльності банків України та вирішення яких вимагає взаємодії органів державної влади та банків України. Участь у дискусії з цього питання науковців і практиків дає змогу виявити низку особливо важливих аспектів, запропонувати аргументовано обґрунтовані рішення, пов'язані з національною і міжнародною правовою регламентацією протидії комп'ютерній злочинності. Необхідно підкреслити велике значення взаємодії правоохоронних органів з банками України з питань ефективної протидії легалізації та відмиванню доходів, одержаних злочинним шляхом за допомогою фінансових інструментів, комп'ютерних мереж, банківських платіжних систем.

Необхідним є вдосконалення законодавчої бази, яка склала б належне юридичне обґрунтовування і довела б необхідність адекватного реагування на виклики кіберзлочинності.

Таким чином, основними проблемами, які вимагають швидкого вирішення, є такі:

- розвиток науково-практичних напрямків, які пов'язані з дослідженнями забезпечення інформаційної безпеки Національного банку України та банків України;
- розробка проекту галузевої нормативно-методичної бази для використання, розробка та розвиток інформаційних систем, які використовуються Національним банком України та банками України;
- розширення співпраці правоохоронних органів з комерційними банками і недержавними організаціями у боротьбі з кіберзлочинністю, а також легалізацією та відмиванням доходів, одержаних злочинним шляхом за допомогою фінансових інструментів, комп'ютерних мереж, банківських платіжних систем;
- вивчення у вищих навчальних закладах питань, пов'язаних з протидією злочинам, які вчиняються з використанням комп'ютерних мереж;
- відкриття інженерної спеціальності з блоку "Комп'ютерні науки" для підготовки фахівців для банківської системи України на базі Севастопольського інституту банківської справи Української академії банківської справи Національного банку України.

В.С. Стельмах,
канд. екон. наук, Голова Національного банку України

Наукове видання

ПРОТИДІЯ ЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ МЕРЕЖ

Тези доповідей Міжнародної
науково-практичної конференції
(Севастополь, 1–2 жовтня 2010 року)

Технічне редагування *І.О. Кругляк*

Комп'ютерна верстка *В.А. Івакін*

Дизайн обкладинки *Ю.М. Хижняк*

Підписано до друку 22.12.2010. Формат 60х90/16. Гарнітура Times.
Обл.-вид. арк. 11,98. Умов. друк. арк. 13,13. Тираж 100 пр. Зам. № 1042

Державний вищий навчальний заклад
“Українська академія банківської справи Національного банку України”
40000, м. Суми, вул. Петропавлівська, 57
Свідоцтво про внесення до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції: серія ДК, № 3160 від 10.04.2008

Надруковано на обладнанні Державного вищого навчального закладу
“Українська академія банківської справи Національного банку України”
40000, м. Суми, вул. Петропавлівська, 57