4. Голосніченко І. П. , Черненко Л. М. Правовий інститут адміністративного оскарження в регулювання діяльності органів державної реєстрації актів цивільного стану / І. П. Голосніченко, Л. М. Черненко // [Електронний ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_ 64.exe? C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_ DOWNLOAD=1&Image_file_name=PDF/VKPI_soc_2012_2_25.pdf

5. Про звернення громадян: Закон України від 2 жовтня 1996 р. // ВідомостіВерховної Ради України. – 1966. – № 47. – Ст. 256.

6. Іващенко О. Ю. Оскарженняадміністративнихпослуг у ВеликійБританії та України (порівняльно-правовийаналіз) / О. Ю. Іващенко: дис. … к.ю.н. / 12.00.07. – К.: Національнаакадеміявнутрішніх справ України, 2012. – 234 с.

7. Власенко Д. О. Адміністративний порядок оскарження рішень, дій чи бездіяльності суб'єктів публічної адміністрації з надання адміністративних послуг / Д. О. Власенко // Політико-правові реформи та становлення громадянського суспільства в Україні : матеріали всеукраїнської науково-практичної конференції (м. Херсон, 10–11 жовтня 2014 року). – Херсон : Видавничій дім «Гельветика», 2014. – С. 98–101.

ДЕЯКІ ПИТАННЯ ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

Ісмайлов К. Ю.
кандидат юридичних наук,
завідувач кафедри кібербезпеки та інформаційного забезпечення
Васильчук О. В.
студент І курсу юридичного факультету
Одеського державного університету внутрішніх справ
м. Одеса, Україна

На сьогодні інформація відіграє особливу роль у процесі розвитку особи, суспільства, державі та всієї цивілізації в цілому. Особлива значимість інформації проявляється саме для банківської сфери, що напряму пов'язана із її специфікою, вже не можливо уявити здійснення банківської діяльності без інформації. Можна стверджувати, що саме грошові кошти та інформація є «двигуном» усієї банківської діяльності.

У сучасних соціально-економічних умовах слід приділяти особливу увагу розвитку фінансової сфери України та важливої її складової – банківської системи. Кожний комерційний банк функціонує не відособлено, а в спільному просторі, і його дії повинні бути узгоджені з інтересами клієнтів, інвесторів, конкурентів, держави. Питання банківської безпеки є актуальним для його власників, акціонерів, оскільки від того, наскільки буде захищеним банк, залежатиме ступінь розвитку бізнесу, рівень отриманого прибутку. Важливу

роль відіграють питання безпеки банку для його клієнтів як уже існуючих, так і майбутніх, особливо вкладників.

Загальними питаннями захисту інформації займались такі вчені, як В.І. Ярочкін, Я.В. Бузанова А.О. Антонюк, Б.А. Кормич та ін. Загальнотеоретичним питанням захисту інформації в банківських установах присвячені роботи Л.М. Стрельбицької, А.Г. Титоренка, М.І. Зубка, Л.В. Ніколаєва, Г.П. Лазарєва, В.О. Хорошко та інших.

Розглядаючи питання банківської безпеки, слід враховувати й партнерів по бізнесу, а також конкурентів, які тісно співпрацюють у межах банківської системи і є взаємопов'язаними.

Важливе місце за таких умов повинно відводитися забезпеченню інформаційної безпеки. Інформаційна безпека – це «системний комплекс взаємопов'язаних запобіжних заходів забезпечення національних інтересів у сфері інформації та інформаційної діяльності; захисту інформаційного суверенітету та інформаційного простору України». У найбільш загальному вигляді системою забезпечення інформаційної безпеки є «сукупність інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення» [1].

Основними напрямами діяльності банківських підрозділів щодо захисту інформації (інформаційної безпеки) є розробка основних напрямів використання технічних та програмних засобів та способів захисту електронної банківської інформації; аналіз та організація діяльності щодо виявлення можливих каналів витоку банківської інформації за допомогою технічних засобів захисту. Заходи щодо забезпечення інформаційної безпеки банку мають бути систематичними і здійснюватися у комплексі з іншими заходами. Важливе значення для забезпечення інформаційної безпеки банківської діяльності має законодавчий рівень такого забезпечення. При розробці системи забезпечення інформаційної безпеки банку особливу увагу потрібно приділяти оцінці відповідності управлінських рішень, технологій, підходів та конкретних програмно-апаратних засобів вимогам чинного законодавства.

Адміністративний рівень інформаційної безпеки реалізується у формі прийнятої політики безпеки, що містить основні принципи та правила, дотримання яких забезпечить цілісність та конфіденційність банківської інформації. Такі принципи та правила політики безпеки містяться у спеціальному документі та відповідних організаційно-розпорядчих документах, які стосуються усіх сфер банківської діяльності і є комплексом управлінських рішень та інструкцій щодо регламентації дій як у звичайному режимі банківської діяльності, так і в екстремальних випадках.

На програмно-технічному рівні застосовується система взаємопов'язаних заходів, які забезпечують ефективну та безпечну роботу серверів безпеки, а також сталу керованість інформаційної системи банку, можливість її розвитку з одночасною протидією новим загрозам при збереженні таких властивостей, як висока ефективність та простота й зручність використання. З метою вико-

нання зазначених вимог здійснюється збір, узагальнення та аналіз інформації з питань перспективного програмно-технічного забезпечення інформаційної безпеки. За результатами такого аналізу з урахуванням вимог Національного банку України вносяться пропозиції щодо впровадження перспективних програмних та технічних засобів захисту в інформаційні системи.

Надійність та ефективність банківської діяльності забезпечується через реалізацію відповідних вимог до системи безпеки (безперервність, плановість, конкретність, активність, універсальність, комплексність), а важливою складовою банківської безпеки є інформаційна безпека.

Інформаційна безпека полягає у формуванні інформаційних ресурсів банку та організації гарантованого їх захисту та досягається створенням у банку системи збору та обробки інформації, проведенням відповідних заходів щодо її зберігання та розподілу, визначенням категорій і статусу банківської інформації, порядку і правил доступу до неї, дотриманням усіма працівниками, клієнтами та акціонерами банку норм і правил роботи з банківською інформацією, своєчасним виявленням спроб і можливих каналів витоку інформації та її перетинанням [2].

Термін «інформаційна безпека» означає «захищеність інформації та підтримувальної інфраструктури від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятних збитків користувачам інформаційних систем, зокрема власникам і користувачам інформаційних ресурсів і підтримувальної інфраструктури» [3]. Виходячи із наведеного, захист банківської інформації є комплексом заходів, спрямованих на забезпечення інформаційної безпеки банку. З методологічної точки зору, порівняльний підхід до проблем інформаційної безпеки банку потрібно починати з виявлення суб'єктів інформаційних банківських правовідносин, їх інтересів, пов'язаних із використанням інформаційних систем банку. В зв'язку з цим представляється, що безпеку банківської діяльності потрібно, насамперед, розуміти як:

– безпеку банку як організації,
– безпеку банківського персоналу,
– безпеку банківських операцій.

Дані напрямки становлять основний комплекс питань забезпечення безпеки будь-якого учасника ринку незалежно від його конкретної діяльності.

Національним банком України з метою підвищення рівня інформаційної безпеки в банківській системі України затверджено Стандарти з управління інформаційною безпекою в банківській системі України: СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD); СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD) [4].

Запровадження Стандартів дозволило по-перше оптимізувати вартість побудови та підтримання системи інформаційної безпеки; по-друге почати відслідковувати та оцінювати ризики в банківській діяльності; по-третє ефективно виявляти найбільш критичні ризики та знижувати ймовірність їх настання; по-

п’яте розробити ефективну політику інформаційної безпеки та забезпечити її якісну реалізацію; по-шосте забезпечити розуміння питань інформаційної безпеки працівниками банку; по-сьоме забезпечити підвищення репутації банку; по-восьме знизити ризики зовнішніх шкідливих впливів для банку.

Інформаційна банківська безпека і захист банківської інформації не є тотожними поняттями, оскільки інформаційна безпека охоплює не тільки поняття захисту, а й аутентифікацію, аудит інформаційних систем, виявлення несанкціонованого проникнення до інформаційної системи банку. Так, наприклад, при передаванні даних з використанням комп’ютерних мереж можуть виникнути проблеми, пов’язані з інформаційною безпекою. Зокрема, якщо банк має територіально відокремлені структурні підрозділи, розташовані на значній відстані один від одного, то при пересиланні інформації загальнодоступною мережею необхідно бути впевненим, що ніхто не зможе скористатися цією інформацією або змінити її. Можуть виникнути проблеми як для банка, так і для його клієнта при розрахунках в Інтернет-магазині, коли оплата відбувається в електронному вигляді. Покупець повинен мати гарантії, що він отримає оплачений товар, відповідно розрахувавшись, а номер його кредитної картки не стане нікому відомий. Тому працівники банківської установи повинні вміти визначати критичні інформаційні ресурси банку та рівень їх захищеності від різних атак, які можуть здійснювати зловмисники або конкуренти, що використовують різні вразливі місця захисту інформаційної системи.

Основними порушеннями інформаційної банківської безпеки, звертають увагу фахівці банківської справи, є втрата конфіденційності (розкриття інформаційних ресурсів), втрата цілісності (їх неавторизована модифікація), втрата доступності (неавторизована втрата доступу до цих ресурсів).

Отже, з метою запобігання порушенням інформаційної безпеки інформаційних банківських ресурсів потрібно постійно виявляти та аналізувати вразливі місця інформаційної системи банку та ресурси, які потребують захисту, а також ймовірні атаки, які можуть відбутися в конкретному оточенні. Після цього потрібно визначити інформаційні ризики для визначеного інформаційного ресурсу, обрати контрзаходи, згідно з обраною політикою банківської безпеки, та забезпечити безпеку за допомогою механізмів і сервісів безпеки. Політика банківської безпеки має визначати взаємопов’язану сукупність механізмів і сервісів безпеки, адекватну ресурсам, що захищаються, і оточенню, в якому їх використовують.

Література:

1. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. ... канд. юрид. наук : 12.00.07 / О. В. Логінов. – К., 2005. – 236 с.

2. Зубок М. І. Організаційно-правові основи безпеки банківської діяльності в Україні : навч. посіб. / М. І. Зубок, Л. В. Ніколаев. – 2-ге вид., допов. – К. : Істина, 2000. – 88 с.

3. Адамик Б.П. Інформаційні технології у банківській сфері : навч. посіб. / Б.П. Адамик, І. С. Литвин, В. О. Ткачук. – К. : Знання, 2008. – 351 с.