УДК 340.13

Тамара Чернадчук,
кандидат юридичних наук,
доцент кафедри адміністративного та інформаційного права
Сумського національного аграрного університету

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОДИН ІЗ НАПРЯМІВ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ*

У статті досліджуються питання, що стосуються забезпечення інформаційної безпеки в сфері банківської діяльності. Звертається увага на виокремлення понять «інформаційна банківська безпека» і «захист банківської інформації». Запропоновано напрями покращення процесу забезпечення інформаційної банківської безпеки.
Ключові слова: *інформаційна безпека, інформаційна банківська безпека, захист банківської інформації.*

У сучасних умовах відбувається розвиток інформаційних процесів, які пронизують усі сфери суспільного життя. Інформатизація сфер суспільного життя стає незворотним процесом, що зобов'язує державу забезпечити стан захищеності суб'єктивних інформаційних прав, а також створювати умови для якісного та ефективного інформаційного забезпечення різних сфер діяльності і, в першу чергу, банківської. 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» [1]. 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» [2].

Сьогодні існують дві тенденції у визначенні поняття інформаційної безпеки. Представники гуманітарного напряму пов'язують інформаційну безпеку тільки з інститутом таємниці, а представники правоохоронних органів пропонують поширювати сферу інформаційної безпеки практично на всі питання і відносини в інформаційній сфері, по суті, ототожнюючи інформаційну безпеку з інформаційним середовищем.

Метою статті є відокремлення понять «інформаційна банківська безпека» і «захист банківської інформації», визначення забезпечення інформаційної банківської безпеки як напрям банківської діяльності та надання пропозицій щодо його покращання.

Б. А. Кормич, досліджуючи організаційно-правові основи політики інформаційної безпеки, слушно звертає увагу на сучасні проблеми обігу комерційної інформації. Проблеми пов'язані з тим, що процес виробництва, розповсюдження та споживання інформації має специфіку, відмінну від аналогічних процесів, що відбуваються з предметами матеріального світу. Ця специфіка полягає в ідеальній природі інформації. На відміну від матеріальних продуктів, споживання яких означає їх руйнування або втрату споживчих якостей, споживання інформації не призводить до аналогічних результатів. Інформація здатна копіюватися скільки завгодно разів, при цьому не зменшуючись і не втрачаючи своїх споживчих якостей. Інформація здатна зберігатися, накопичуватися на будь-яких, придатних для цього носіях, а також у свідомості як окремого індивідуума, так і в масовій свідомості суспільства. Інформація здатна змінюватися, вдосконалюватися, деталізуватися; на її основі мож-

* Рекомендовано до друку кафедрою адміністративного та інформаційного права Сумського національного аграрного університету.

ливе створення нової інформації тощо. Суб'єкт, що отримав, спожив інформацію, може передавати її іншим суб'єктам або в незмінному вигляді, або переробивши її завдяки власному розуму, або створивши нову інформацію. При цьому в процесі передачі або поширення інформації вона, будучи отриманою іншими суб'єктами, залишається і у суб'єкта, що її поширює [3].

Сучасний розвиток суспільних відносин, і в першу чергу ринкових, зумовлює необхідність забезпечення правового захисту інформації в сфері обігу грошових коштів, зокрема при здійсненні банківських операцій. Відносини між банком та клієнтом у силу специфіки банківської діяльності мають довірчий характер. Клієнт не лише довіряє банку свої грошові кошти, а й потенційно допускає його до інформації про свій фінансовий стан. Розголошення відомостей, що стосуються фінансового стану клієнта і особливо відомостей, що становлять банківську таємницю, може негативно вплинути на безпеку та репутацію клієнта банку, що підсилює необхідність чіткого державного регулювання інформаційної сфери банківської діяльності.

Проблемою сучасного законодавства, що регулює інформаційні відносини у сфері банківської діяльності, є відсутність системності у визначенні поняття банківської таємниці, відсутність законодавчого визначення поняття банківської інформації, її чіткої класифікації та встановлення правового режиму кожного виокремленого виду банківської інформації. За чисельністю значень і функцій, які може мати інформація при обігу в соціальних системах, вона може виступати не лише як джерело інформування про події та явища банківсько-правової дійсності та отримання знань, а й як таємниця, за посередництвом якої обмежується доступ до інформації, отримують захист державні та комерційні секрети. Ще однією проблемою можна визнати необхідність вироблення єдиного підходу в уточненні права на банківську інформацію і особливо банківську таємницю як особливого комплексного інституту, підстав та порядку обмеження права на банківську таємницю, охорони та захисту цього права при здійсненні повноважень власниками та користувачами банківської таємниці.

У сучасних умовах виникають нові напрями банківської діяльності, зокрема забезпечення банківської безпеки. Поряд із завданнями забезпечення основної кредитно-фінансової діяльності виникають особливі завдання щодо захисту інтересів банку шляхом виконання функцій забезпечення банківської безпеки, які спрямовані на попередження або зниження тяжких наслідків протиправних дій проти банку [4]. Такий висновок зумовлений тим, що в сучасних умовах розвитку інформаційних технологій загрозу для банку становлять так звані «інтелектуальні шахраї», які використовують у своїй діяльності досягнення сучасних технологій. Тому на сучасному етапі розвитку суспільства можливо ототожнення банківської безпеки передусім із захистом від інтелектуальних атак.

У працях, присвячених організаційно-правовим питанням безпеки банківської діяльності, виділяють, крім особистої, колективної та економічної безпеки, й інформаційну безпеку банку, яка забезпечує формування інформаційних ресурсів банку та організації їх захисту [5].

Ризик заподіяння збитків від шахрайства в сфері кредитування може бути значно меншим завдяки здійсненню сукупності заходів, зокрема: перевірка достовірності відомостей та документів, що засвідчують право особи укладати договір в обсязі та на умовах, передбачених проектом договору; отримання відомостей, що підтверджують існування особи-позичальника шляхом дослідження установчих документів, відомостей, отриманих з податкових та інших органів, а також здійснення інших заходів щодо збору та аналізу даних стосовно позичальника.

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 виконання 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 [6].

На думку інших науковців, 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» [7]. 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.

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) [8]. Запровадження Стандартів дозволить оптимізувати вартість побудови та підтримання системи інформаційної безпеки; відслідковувати та оцінювати ризики в банківській діяльності; ефективно виявляти найбільш критичні ризики та знижувати ймовірність їх настання; розробити ефективну політику інформаційної безпеки та забезпечити її якісну реалізацію; забезпечити розуміння питань інформаційної безпеки працівниками банку; забезпечити підвищення репутації банку; 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-крамниці, 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) [9].

Отже, з метою запобігання порушенням інформаційної безпеки інформаційних банківських ресурсів потрібно 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.

ПРИМІТКИ

1. Шадрин И. П. Подготовка и принятие управленческого решения / И. П. Шадрин. — Якутск, 1970. — 123 с.
2. 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.
3. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра юрид. наук : 12.00.07 / Борис Анатолійович Кормич. — О., 2004. — 427 с.
4. Побережный С. Н. Модели и методы обеспечения банковской безопасности : монография / С. Н. Побережный, Б. А. Дадашев, А. Л. Пластун. — Сумы : ГВУЗ «УАБД НБУ», 2010. — 239 с.
5. Зубок М. І. Організаційно-правові основи безпеки банківської діяльності в Україні : навч. посіб. / М. І. Зубок, Л. В. Ніколаєв. — 2-ге вид., допов. — К. : Істина, 2000. — 88 с.
6. Там само.
7. Адамик Б. П. Інформаційні технології у банківській сфері : навч. посіб. / Б. П. Адамик, І. С. Литвин, В. О. Ткачук. — К. : Знання, 2008. — 351 с.
8. Постанова Правління НБУ № 474 від 28.10.2010 р. «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України» [Електронний ресурс]. — Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=v0474500-10.
9. Адамик Б. П. Зазнач. праця.

Чернадчук Тамара. Обеспечение информационной безопасности как одно из направлений банковской деятельности.
В статье исследуются вопросы, касающиеся обеспечения информационной безопасности в сфере банковской деятельности. Обращается внимание на выделение понятий «информационная банковская безопасность» и «защита банковской информации». Предложены направления улучшения процесса обеспечения информационной банковской безопасности.
Ключевые слова: *информационная безопасность, информационная банковская безопасность, защита банковской информации.*

Chernadchuk Tamara. Providing information security as one of the areas of banking activity.
The article investigates the issues of information security in the banking sphere. Attention is paid to the selection of concepts of information security and the protection of banking information. Directions of improving the process of ensuring the information security of the banking.
Key words: *information security, banking information security, protection of banking information.*