Фізико-математичні науки

УДК 65.51

Савчук Олександр Васильович

аспірант

Національного університету «Острозька академія»

Savchuk Oleksandr

Postgraduate Student of the

National University of Ostroh Academy

ЗАГРОЗА ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ БАНКУ З ВРАХУВАННЯМ ЛЮДСЬКОГО ЧИННИКА
THE THREAT OF BANK CONFIDENTIAL INFORMATION LEAK TAKING INTO ACCOUNT OF HUMAN FACTOR

Анотація. *У статті представлено опис важливості захисту конфіденційної інформації банківських установ, розглянуто нормативно-правову базу, що регулює поняття конфіденційності, описано відмінності між комерційною таємницею та банківською таємницею. Також описано важливість людського фактору у інформаційній безпеці банківських установ, розглянуто математичну модель, що дозволяє визначити можливість витоку конфіденційної інформації, яка опирається на людські чинники.*

Ключові слова: *конфіденційна інформація, банківська таємниця, комерційна таємниця, людський фактор, математична модель.*

Summary. *The article describes the importance of protecting the confidential information of banking institutions, considers the legal framework governing the concept of confidentiality, and describes the differences between trade secrets and banking secrets. The importance of the human factor in the information security of banking institutions is also described, and a mathematical*

model is considered, which allows determining the possibility of leakage of confidential information based on human factors.

Key words: *confidential information, banking secrecy, trade secrecy, human factor, mathematical model.*

Постановка проблеми. Зараз відбувається активний розвиток фінансово-кредитної сфери держави. Основною складовою економіки держави є банківська система, і вона повинна бути надійно захищеною. Для її нормального функціонування необхідний високий рівень довіри як юридичних, так і фізичних осіб. Необхідно забезпечити безпеку інформації, яка являє собою комерційну таємницю, зокрема банківську комерційну таємницю. Для цього слід вдосконалювати існуючі організаційні та нормативно-правові документи, що дозволять регулювати інформаційну безпеку. Проте, слід також звернути увагу на психологічні особливості людей, що є головним джерелом порушень конфіденційності цієї інформації. Можливість змоделювати поведінку працівників, коли до них потрапляє конфіденційна інформація, є необхідною процедурою, що дозволить уникнути, або й навіть передбачити подібні інциденти.

Аналіз останніх досліджень та публікацій. Питання конфіденційної інформації є досить актуальним та визначається глобальною роллю самої інформації на сучасному етапі соціально-економічного розвитку суспільства, визнанням її як майнової та немайнової цінності для окремої особи, суспільства чи держави в цілому. Інформаційні ресурси є досить цінним товаром на ринку, у тому числі і міжнародному, який можна співставити за економічними показниками із фінансовими, природними та іншими ресурсами. Теоретичним описом понять конфіденційності інформації займалась велика кількість науковців, зокрема з галузей правознавства та кібербезпеки. В основному, ці галузі комбінуються у наукових роботах, так як доцільніше розглядати комплексно. Так, Гоголь Б.

пропонує розрізняти поняття конфіденційної інформації та комерційної таємниці [1], Решетілова О. та Граб Т. описують можливості регулювання конфіденційності інформації у трудових відносинах [2], а Табаков В. пропонує математичну модель для врахування людського чинника при побудові систем захисту інформації [3].

Виклад основного матеріалу. Інформація є ключовим фактором розвитку різноманітних сфер діяльності, у тому числі й у банківській сфері. У будь-якого банку вона вважається найбільш цінним ресурсом, оскільки використовується для реалізації певних цілей. Інформація може бути як відкритою, так і закритою. Відкрита інформація знаходиться у вільному доступі, а закрита інформація знаходиться у обмеженому доступі та є конфіденційною.

У статті 21 Закону України «Про інформацію» зазначено, що конфіденційна інформація – це інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [4]. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Конфіденційна інформація, яку мають у власному розпорядженні банківські установи, складається із комерційної та банківської таємниці. Хоча ці поняття і мають досить значну відмінність, проте їх захист займає пріоритетне місце у банківській діяльності.

Відповідно до статті 505 Цивільного Кодексу України, комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи у певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною інформацією можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [5].

Комерційна таємниця тісно пов'язана із банківською таємницею. Її захист є однією із найважливіших завдань держави, так як фінансова сфера відіграє ключову роль у розвитку економіки. Банківська таємниця також є дотичною до політичних проблем, оскільки останнім часом у державі виникає велика кількість питань щодо відмивання грошей, в тому числі й у іноземних банках, відтоку капіталу тощо.

Згідно статті 60 Закону України «Про банки та банківську діяльність», 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, є банківською таємницею. Вона, як певний вид інформації з обмеженим доступом, покликана охороняти відомості, вільний обіг яких може порушити права та інтереси клієнтів банку [6].

Комерційна таємниця в банку та банківська таємниця мають спільні елементи та тісно пов'язані між собою. Однак, вони відрізняються за об'єктами інформації. В банківській таємниці об'єктом є саме банківські дані, які важливі для клієнта (дані про рахунки чи вклади, особисті дані клієнта та ін.). У комерційній таємниці об'єктом виступає інформація, яка, більшою мірою, пов'язана із самим банком (дані про контрагентів та конкурентів, дані про структуру управління і т.д.). На основі цього, можна зробити висновок, що банківська таємниця направлена на захист інформації, яка є цінною для клієнта. Комерційна таємниця в банку, навпаки, направлена на захист інформації, яка важлива для самого банку. Хоча, незважаючи на це, обидва види таємниць є конфіденційною інформацією банку.

На державному рівні захист конфіденційної інформації в банку забезпечується за рахунок створення нормативно-правових актів, в рамках яких зобов'язані працювати фінансові установи. На сьогодні немає окремого спеціального закону, який стосувався би правової охорони конфіденційної інформації. Регулювання правових відносин, що стосуються її, здійснюються на основі положень Цивільного Кодексу України, Господарського Кодексу України, Кримінального Кодексу України, Законів України «Про інформацію», «Про доступ до публічної інформації», «Про захист від недобросовісної конкуренції» та іншими нормативно-правовими актами. У зв'язку з цим, банківські установи повинні забезпечувати захист як на правовому, так і на технічному рівні.

Банківські установи, в основному, опираються на задіяні технічні рішення щодо захисту конфіденційної інформації. Їх впровадження є виправданим, адже захист інформації в банку має бути на досить високому рівні, аби відбивати усі атаки та спроби проникнення з боку злочинців. Для мінімізації фінансових та репутаційних ризиків необхідно захистити не тільки бази даних та робочі станції персоналу, але також і комп'ютерні мережі, термінали працівників фронт-офісів а також банкомати від шкідливого впливу. Важливо розуміти, що всього лиш одна використана злочинцем вразливість може призвести до успішної кібератаки на організацію, так як фінансові сервіси взаємопов'язані і із ланцюжка одиночних атак, які не являють собою значної небезпеки в кожному окремому випадку, можна здійснити успішне проникнення до критично важливих систем.

Сьогодні найбільш поширеними є три способи крадіжки конфіденційної інформації. По-перше, фізичний доступ до місць її зберігання та обробки. Тут існує багато варіантів. Наприклад, зловмисники можуть проникнути до офісу банку і викрасти жорсткі диски з усіма базами даних. Можливим є також збройний грабіж, ціллю якого є не гроші, а

інформація. Не включається і ситуація, коли працівник самостійно може винести носій інформації поза межі території.

По-друге, використання резервних копій. У більшості банків системи резервування важливих даних побудовані таким чином, аби записувати частину важливої інформації на нові носії та зберігати їх окремо. Доступ до них регламентується менш жорсткий, аніж доступ до основних даних. При їх транспортуванні та зберіганні відносно велика кількість людей може зняти з них копії, або ж напряму заволодіти ними.

По-третє, найбільш ймовірний спосіб витоку конфіденційної інформації – несанкціонований доступ працівниками банку. При використанні для розподілу прав тільки стандартних засобів операційних систем у користувачів нерідко виникає можливість опосередковано повністю скопіювати бази даних, з якими вони працюють, та винести їх за межі установи. Іноді працівники роблять це без усілякого злого умислу, просто щоби працювати з цією інформацією з дому. Однак, такі дії є серйозним порушенням політики безпеки та можуть стати причиною розголошення конфіденційної інформації.

Останні дослідження в області інформаційної безпеки, наприклад щорічний випуск Internet Crime Report від Федерального Бюро Розслідувань [7], показали, що фінансові втрати компаній від більшості загроз щороку знижуються. Однак, є декілька ризиків, від яких збитки тільки зростають. Один з них – крадіжка конфіденційної інформації або ж порушення прав поводження з нею тими працівниками, доступ яких до конфіденційних даних необхідний для виконання службових обов'язків. Таких працівників називають інсайдерами.

Ефективним засобом мінімізації ризиків, пов'язаних з інсайдерами, є спеціальне програмне забезпечення, що здійснює динамічне управління усіма пристроями та портами комп'ютера, які можуть бути використані для копіювання інформації. Їх принцип дії наступний: для кожної групи

користувачів або для кожного користувача окремо задаються дозволи на використання певних портів та пристроїв. Найбільшою перевагою такого ПЗ є гнучкість. Вводити обмеження можна для конкретних типів пристроїв, їх моделей та окремих екземплярів. Це дозволяє вводити досить складні політики розподілення прав доступу.

Як правило, працівники є найменш надійною складовою системи захисту інформації. Для боротьби з цим фактором банки зачасту використовують наступні методи та засоби захисту конфіденційної інформації щодо власних працівників [8]:

- ознайомлюють усіх працівників з принципами захисту інформації та принципами роботи засобів зберігання та обробки інформації;
- чітко класифікують всю інформацію за ступенем її закритості та вводять правила поводження з документами обмеженого доступу;
- зобов'язують працівників дотримуватись вимог захисту інформації, підкріплюючи це відповідними організаційними та правовими нормами;
- навчають усіх працівників сучасним засобам захисту інформації;
- наймають в штат спеціаліста, що професійно працює з проблемами інформаційної безпеки;
- проводять навчальні психологічні тренінги, які сприяють напрацюванню у працівників певних алгоритмів відповіді на компрометуючі питання, при яких можливий витік інформації;
- здійснюють контроль, моніторинг та аудит діяльності працівників;
- забезпечують відповідальність за несанкціоноване розголошення конфіденційної інформації.

У зв'язку з тим, що людський фактор є ключовим при витоці конфіденційної інформації, - доцільно звернути увагу на шляхи попередження цьому, які не включені у вище перелічені заходи. У абсолютній більшості випадків уся конфіденційна інформація, що витікає з

банківських установ, продається на чорному ринку. Конфіденційна інформація виступає товаром, яким торгують, і, як і будь-який товар, ця інформація має власну ціну.

В. Табаков запропонував математичну модель [3], яка дозволяє змоделювати ситуацію, як можна запобігти витоку конфіденційної інформації з вини працівників шляхом правильного регулювання політики оплати праці в установі. Суть моделі полягає у припущенні, що працівник продає інформацію за значно нижчою ціною, ніж вона вартує в дійсності, особливо якщо не знає її. Покупець цієї інформації є досить обізнаним про неї та пропонує за неї певну ціну X. У цьому випадку прибуток $V(q_i X)$ і-го працівника (продавця конфіденційної інформації), можна оцінити наступним чином:

$$V(q_i X) = X - p_{1i}\big(nD(q_i) + lB(q_i)\big) - p_{2i}R(q_i), \quad (1)$$

де p_{1i} – ймовірність викриття продавця; n – кількість місяців, які пропрацював би на фірмі продавець без цього правопорушення; $D(q_i)$ – місячний оклад працівника; l – кількість отриманих премій; $B(q_i)$ – розмір премій; p_{2i} – ймовірність збитку у разі викриття; $R(q_i)$ – розміри морального та матеріального збитку, виражені у грошовому еквіваленті.

Прибуток покупця $\pi(q_i X)$ можна оцінити наступним чином:

$$\pi(q_i X) = k(q_i)C(q_i) - X - S(q_i) - p_{3i}U(q_i), \quad (2)$$

де $k(q_i)C(q_i)$ – «продажна ціна» блоку інформації; $S(q_i)$ – засоби, витрачені на вербування продавця; p_{3i} – ймовірність викриття покупця; $U(q_i)$ – матеріальні та моральні втрати внаслідок викриття, виражені у грошовому еквіваленті.

З моделі прибутку продавця (1) випливає, що для нього прийнятною ціною за товар є ціна, що задовольняє вимозі:

$$X > p_{1i}\big(nD(q_i) + lB(q_i)\big) + p_{2i}R(q_i) \quad (3)$$

З моделі прибутку покупця (2) випливає, що для нього прийнятною ціною за товар є ціна, що задовольняє вимозі:

$$X \leq k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i) \quad (4)$$

Таким чином, для покупця прийнятною ціною за товар є ціна, яка знаходиться у сегменті компромісу:

$$[p_{1i}\big(nD(q_i) + lB(q_i)\big) + p_{2i}R(q_i), k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i)] \quad (5)$$

Звідси автор зробив висновок, який полягає у тому, що для виключення витоку та продажу конфіденційної інформації достатньою умовою є наступна:

$$p_{1i}\big(nD(q_i) + lB(q_i)\big) + p_{2i}R(q_i) > k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i) \quad (6)$$

Тобто, діють звичайні ринкові відносини, коли існує товар у вигляді конфіденційної інформації, продавець, як недобросовісний працівник банку що може заволодіти товаром та здійснювати його подальший продаж, та покупець, що використовуватиме придбаний товар задля власної вигоди. У торгівлі, для того щоб інший покупець не отримав товар від продавця, слід запропонувати ціну, вигіднішу для нього. Відповідно до пропонованого автором висновку (6), для того, аби витік конфіденційної інформації не відбувся, працівник банку повинен отримувати винагороду за власну працю, що буде еквівалентною або ж навіть більшою, аніж пропонуватиме покупець.

Висновки. Важливість нормативно-правового регулювання конфіденційності інформації у будь-якій установі повинно відігравати ключову роль. А у банківській установі це має бути базовою ціллю для повноцінного функціонування. Розглянуті особливості поняття конфіденційної інформації, розрізнення понять комерційної та банківської таємниці дозволяють осягнути суб'єктну базу необхідності захисту цієї інформації. Побудова практичних рішень для інформаційної безпеки банківських установ є комплексним процесом, що опирається на ці поняття та, проте, не дозволить повністю задовольнити відведену їм роль. Це

підтверджується тим, що витоки конфіденційної інформації стаються постійно, хоч динаміка їх виникнення дещо сповільнюється останнім часом. Практичним рішенням до покращення цієї ситуації є ширший погляд на саму проблему витоку інформації. Йдеться саме про людський чинник, що є рушійною силою для виникнення подібних подій. Розглянута у роботі математична модель, при інтеграції її у створену систему захисту інформації, дозволяє звертати увагу саме на подібні проблеми. Таким чином, у роботу щодо створення та вдосконалення існуючих систем захисту банківської конфіденційної інформації повинен бути інтегрований саме людський фактор, як першопричина проблеми.

Література

1. Гоголь Б. М. Комерційна таємниця та конфіденційна інформація: окремі проблеми співвідношення / Б. М. Гоголь. // Кібербезпека та інтелектуальна власність: проблеми правового забезпечення. 2017. №1. С. 112–116.
2. Решетілова О. М. Забезпечення захисту конфіденційної інформації і комерційної таємниці в трудових відносинах / О. М. Решетілова, Т. В. Граб. // Вчені записки кафедри документознавства та інформаційної діяльності. 2019. №1. С. 70–73.
3. Табаков В. З. Математична модель витікання конфіденційної інформації з урахуванням людського чинника / В. З. Табаков. // Математика та кібернетика – фундаментальні та прикладні аспекти. 2011. №2. С. 29–30.
4. Закон України "Про інформацію" [Електронний ресурс] // Відомості Верховної Ради України (ВВР). 1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Цивільний кодекс України [Електронний ресурс] // Відомості Верховної Ради України (ВВР). 2003. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text
6. Закон України "Про банки і банківську діяльність" [Електронний ресурс] // Відомості Верховної Ради України (ВВР). 2001. URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text
7. Internet Crime Report [Електронний ресурс] // Federal Bureau of Investigation. 2022. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
8. Вимоги до роботи з конфіденційною інформацією установи // Баланс-Бюджет. 2020. №50.