В. В. Капустинська,
здобувачка першого (бакалаврського) рівня вищої освіти,
спеціальності 072 «Фінанси, банківська справа та страхування»
освітньої програми «Банківська справа»;
науковий керівник
К. О. Кірєєва,
кандидат економічних наук,
доцент кафедри банківської справи;
Державний торговельно-економічний університет

БЕЗПЕКА БАНКУ В УМОВАХ ЦИФРОВІЗАЦІЇ

Цифрові технології стали невід'ємною частиною сучасного світу, змінюючи способи, за допомогою яких люди ведуть свої фінансові операції. Однак ця цифрова трансформація вносить і нові виклики для банківської безпеки. У зв'язку з цим, забезпечення фінансової безпеки стає дуже важливим для банків в умовах цифровізації.

Питання фінансової безпеки банку є досить дискусійним, і кожен вчений трактує дане поняття по різному.

А. Епіфанов [1] та Т. Болгар [2] вважають, що фінансова безпека банку – це стан банківської установи, що характеризується збалансованістю та стійкістю до впливу зовнішніх і внутрішніх загроз, його здатністю досягати поставлених цілей і генерувати достатній обсяг фінансових ресурсів для забезпечення сталого розвитку.

На думку Барановського О. І. сукупність умов, за яких потенційно небезпечні для фінансового стану комерційного банку дії чи обставини попереджені чи зведені до такого рівня, за якого вони не здатні завдати шкоди встановленому порядку функціонування банку, збереженню й відтворенню його майна і перешкодити досягненням банком статутних цілей; стан захищеності фінансових інтересів комерційного банку, його фінансової стійкості, а також середовища, в якому він функціонує [3].

На нашу думку, фінансова безпека банку – це забезпечення стійкості та надійності фінансових операцій та процесів, які відбуваються у банку. Загальна мета фінансової безпеки банку полягає в забезпеченні стабільності, надійності та довіри до його діяльності, що є важливим для успішного функціонування та розвитку банківської системи.

В процесі ведення своєї діяльності в умовах цифровізації, банки стикаються з рядом зовнішніх загроз, які становлять небезпеку для функціонування банку:

- кібератаки, які включають хакерські атаки, що можуть призвести до несанкціонованого доступу до даних банку та віруси і шкідливе програмне забезпечення.
- фішинг та соціальна інженерія

• DDoS-атаки – атаки, під час яких зловмисники намагаються перевантажити мережеві ресурси банку, змушуючи їх працювати некоректно або навіть призводячи до тимчасового припинення роботи банку.

Крім зовнішніх загроз банку, небезпеку для банку можуть становити і внутрішні загрози. До них, насамперед, відноситься персоналу банку. Дії працівників банку, в контексті несення загрози, можуть бути умисними та неумисними. Умисними діями працівника банку може стати рішення використовувати конфіденційну інформацію банку для особистої вигоди або з метою шкоди для банку. Неумисними вважаються дії працівника, в результаті некоректного використання технологій або недбалого відношення до безпекових процедур, може стати причиною витоку конфіденційної інформації або інших безпекових порушень.

Подолання вищенаведених загроз фінансової безпеки банку в умовах цифровізації вимагає комплексного підходу та застосування різноманітних стратегій та технологій. *Серед заходів захисту безпеки, які банку доцільно провадити в своїй діяльності, варто виокремити:*

1. Зміцнення кібербезпеки:

• Впровадження сучасних систем мережевої безпеки, таких як мережеві брандмауери, інтра і екстра-мережеві моніторингові системи, що допомагають виявляти та блокувати небажані атаки.

• Використання шифрування для захисту конфіденційної інформації від несанкціонованого доступу.

2. Навчання та освіта:

• Проведення регулярних тренінгів з кібербезпеки для персоналу банку та надання освітніх матеріалів клієнтам щодо захисту їхніх особистих фінансових даних.

• Підвищення усвідомленості стосовно потенційних кіберзагроз серед персоналу та клієнтів, щоб вони могли розпізнати та запобігти атакам.

3. **Регулярні аудити та моніторинг:**

• Проведення регулярних аудитів безпеки для виявлення слабких місць у системі та внесення відповідних змін для підвищення захисту.

• Постійний моніторинг мережі та систем на предмет підозрілих активностей та невідповідностей, що дозволяє вчасно реагувати на можливі загрози.

4. Використання інноваційних технологій:

• Використання алгоритмів штучного інтелекту для виявлення аномальних патернів поведінки та вчасної реакції на потенційні загрози.

• Використання блокчейну для створення безпечних та недоступних до вторгнення систем збереження даних та виконання фінансових транзакцій.

5. Співпраця з іншими суб'єктами:

• Співпраця з іншими банками, органами правопорядку та кібербезпековими експертами для обміну інформацією про виявлені кіберзагрози та розробки спільних стратегій захисту.

У світі швидко зростаючих цифрових технологій фінансова безпека банку стає важливішою ніж будь-коли. Забезпечення стійкості, конфіденційності та надійності фінансових операцій та даних – це основна вимога для збереження довіри клієнтів і стабільності банку.

Для успішного подолання загроз фінансовій безпеці банку в умовах цифровізації необхідно вжити комплексних заходів, включаючи зміцнення кібербезпеки, навчання персоналу та клієнтів, регулярні аудити та моніторинг, використання інноваційних технологій та співпрацю з іншими суб'єктами.

Лише через постійне удосконалення та адаптацію до змін в кіберпросторі банки зможуть забезпечити високий рівень фінансової безпеки та зберегти довіру клієнтів і стабільність своєї діяльності в умовах цифрової трансформації.

Список використаних джерел

1. Єпіфанов А. О. Фінансова безпека підприємств і банківських установ : монографія. Суми : ДВНЗ «УАБС НБУ, 2009. 295 с.

2. Болгар Т. М. Фінансова безпека банків в умовах ринкової трансформації економіки України : автореф. дис. … канд. екон. наук : 08.00.08. Суми : ДВНЗ «УАБС НБУ», 2009. 22 с

3. Барановський О. І. Банківська безпека: проблема виміру. Економіка і прогнозування. 2006. № 1. С. 7–26.