Юрій Фурдас, Світлана Яцишин*
[1]аспірант кафедри КН, НЛТУ України, Львів, Україна.
furdas.iurii@nltu.edu.ua.
[2]завідувач кафедри ІПЗ НЛТУ України, к.т.н., доцент, Львів, Україна.
https://orcid.org/0000-0001-5200-4837, yatsyshyn@nltu.edu.ua.

Аналіз ризиків інформаційної безпеки в банківській системі

Анотація. Дослідження присвячене вивченню сучасних методів та технологій для ідентифікації, оцінки та управління ризиками в банківському секторі. Враховуючи високий рівень конфіденційності фінансових даних та критичну важливість безперервності банківських операцій, банківська система є одним з найбільш вразливих секторів для кібератак. Основна увага в дослідженні приділяється виявленню основних загроз, таких як фінансове шахрайство, внутрішні загрози, фішинг, DDoS-атаки, а також вразливості інформаційних систем банків. Окрім технічних аспектів, розглядаються також регуляторні вимоги, такі як PCI DSS, що впливають на безпеку платіжних операцій та зобов'язують банки дотримуватися високих стандартів захисту даних. Висвітлено значення автоматизації та інтеграції технологій для зменшення людських помилок та підвищення швидкості реагування на інциденти.

Ключові слова – загроза, кібератака, ризики, інформаційна безпека.

Аналіз ризиків інформаційної безпеки в банківській системі передбачає використання сучасних технологій для моніторингу загроз, автоматизації процесів реагування та оцінки вразливостей [1]. Інтеграція інструментів, таких як SIEM і SOAR. Використання SIEM (системи управління інформаційною безпекою та подіями) та SOAR (системи оркестрації, автоматизації та реагування на інциденти) забезпечує проактивне виявлення кібератак і знижує кількість інцидентів, пов’язаних з людськими помилками. Дослідження показують (https://csecurity.kubg.edu.ua/index.php/journal/article/view/646), що використання штучного інтелекту і машинного навчання для аналізу великих даних дає змогу банківським установам покращити виявлення фінансового шахрайства, зменшити час реагування на загрози та підвищити загальну стійкість до кібератак. Особлива увага приділяється розробці індивідуальних моделей управління ри-

* науковий керівник

зиками, що базуються на оцінці критичних інформаційних активів банків та їх відповідності регуляторним вимогам, таким як PCI DSS [4]. PCI DSS (Payment Card Industry Data Security Standard) – це глобальний стандарт безпеки, розроблений для захисту даних платіжних карток. Він застосовується до будь-якої організації, яка приймає, зберігає, передає або обробляє платіжні картки (враховуючи банки, інтернет-магазини, процесингові центри тощо). Аналіз ризиків є важливим процесом, оскільки банки зберігають велику кількість конфіденційних даних та виконують операції, які можуть бути вразливими до кібератак. Нижче розглянуто основні аспекти цього аналізу.

Можна виділити наступні основні загрози для банківських систем [2]:

Фінансові шахрайства - це неправомірні дії, спрямовані на отримання вигоди через обман, зловживання довірою чи підробку. Вони можуть мати різні форми та масштаби, і часто вражають як окремих споживачів, так і великі компанії. Кіберзлочинці можуть намагатися отримати несанкціонований доступ до банківських систем для викрадення коштів, зміни фінансових транзакцій або викрадення особистих даних клієнтів.

Phishing - це форма шахрайства, при якій злочинці намагаються отримати особисту інформацію, наприклад, логіни, паролі або дані кредитних карток, видаючи себе за законні організації. Це може бути реалізовано через електронні листи, повідомлення в соціальних мережах або навіть текстові повідомлення. Соціальна інженерія - це більш широкий термін, який охоплює будь-які методи маніпуляції людьми для отримання конфіденційної інформації або доступу до систем Ці методи використовуються для обману співробітників або клієнтів з метою отримання облікових даних або іншої конфіденційної інформації.

DDoS-атаки - це вид кібератак, спрямованих на перевантаження серверів, мереж або служб, щоб вони стали недоступними для користувачів. Атака виконується шляхом надсилання великої кількості запитів на сервер з різних комп'ютерів (зазвичай інфікованих шкідливим програмним забезпеченням), що створює "дозування" трафіку, яке перевищує можливості системи обробляти легальні запити. Напади, спрямовані на перевантаження банківських серверів, мо-

* науковий керівник

жуть тимчасово блокувати доступ до онлайн-банкінгу, що може призвести до значних фінансових втрат.

Внутрішні загрози - це ризики, які походять зсередини організації і можуть призвести до втрати або компрометації інформації. Вони можуть бути результатом свідомих або несвідомих дій співробітників, порушення політик безпеки або навіть технічних збоїв. Неналежна поведінка або помилки з боку співробітників також можуть призвести до витоку даних або ненавмисних дій, які загрожують безпеці.

Методи аналізу ризиків. Оцінка вразливостей - є критично важливим етапом у методах аналізу ризиків, який дає змогу виявити слабкі місця в системі інформаційної безпеки. Цей процес передбачає ідентифікацію, аналіз та оцінку вразливостей, щоб зрозуміти, як вони можуть бути використані зловмисниками. Містить аналіз систем на наявність відомих вразливостей, таких як відсутність актуальних оновлень безпеки або неправильно налаштовані системи доступу.

Аудит доступу до інформаційних ресурсів - це процес перевірки, оцінки та аналізу прав доступу користувачів до інформаційних систем і даних. Він допомагає виявити можливі ризики, забезпечити дотримання політик безпеки та виявити неналежні або надмірні права доступу, які можуть призвести до витоку або втрати даних. Аналіз того, хто має доступ до критичних систем і даних, і чи відповідає цей доступ політикам безпеки.

Моніторинг аномалій у мережі: є важливим елементом забезпечення інформаційної безпеки, оскільки дає змогу виявляти та реагувати на потенційні загрози в режимі реального часу. Аномалії можуть свідчити про шкідливу активність, таку як кібератаки, витоки даних або внутрішні загрози. Використання інструментів для виявлення аномальної активності в банківських мережах, таких як незвичні транзакції або спроби несанкціонованого доступу.

Впровадження технологій для управління ризиками. SIEM-системи-SIEM (Security Information and Event Management) - це технологія, що поєднує в собі управління інформаційною безпекою та управління подіями для забезпе-

* науковий керівник

чення захисту інформаційних систем. Вона дає змогу організаціям збирати, зберігати, аналізувати та реагувати на дані безпеки в реальному часі. У банках використовуються SIEM для аналізу логів, виявлення загроз та формування попереджень у реальному часі.

Штучний інтелект (ШІ) і машинне навчання (МН) стали важливими інструментами для управління ризиками в інформаційній безпеці. Вони здатні обробляти великі обсяги даних, виявляти патерни та автоматизувати процеси, що значно підвищує ефективність захисту інформаційних систем Застосування цих технологій дає змогу виявляти шахрайські дії та аномалії в даних швидше, ніж це може зробити людина.

Шифрування даних - це процес перетворення інформації в незрозумілий формат, що робить її недоступною для несанкціонованого доступу. Воно є важливим елементом забезпечення інформаційної безпеки, особливо в контексті захисту конфіденційних даних в організаціях, зокрема у банківських системах. Ключовий інструмент для захисту конфіденційної інформації клієнтів, що забезпечує збереження даних навіть у випадку несанкціонованого доступу.

Регуляторні вимоги. Банківська система підпадає під суворі вимоги до інформаційної безпеки, встановлені національними та міжнародними регуляторами:

- Національний банк України – Регулювання інформаційної безпеки. Положенням НБУ № 95 "Про організацію системи управління інформаційною безпекою"[5];
- PCI DSS (Payment Card Industry Data Security Standard) зобов'язують банки дотримуватися високих стандартів у сфері захисту платіжних карт [4];
- ISO/IEC 27001 – це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (СУІБ) [6].

Автоматизація аналізу ризиків. В умовах постійно зростаючої кількості загроз автоматизація процесів аналізу ризиків та реагування на інциденти стає важливою частиною захисту. Використання SOAR-систем для автоматизації

* науковий керівник

реагування на інциденти та впровадження механізмів оркестрації дає змогу зменшити час на виявлення і нейтралізацію загроз. Серед переваг автоматизації: зменшення людських помилок - автоматизовані рішення мінімізують вплив людського фактора, що є однією з основних причин інформаційних витоків. Підвищення швидкості реагування - завдяки автоматизації процеси виявлення загроз і реагування на них виконуються набагато швидше.

Аналіз великих даних - сучасні інструменти дають змогу обробляти великі обсяги даних, що неможливо зробити вручну, та генерують важливі аналітичні висновки для управління ризиками.

Розрахунок оцінки ризику можна виконувати за наступною формулою:

$$N=S*O*D, \quad (1)$$

де N – Номер пріоритету ризику, S – Серйозність, O – Виникнення; D – Виявлення.

Цей базовий розрахунок дає змогу організаціям швидко отримувати знімки різних ризиків для легкого порівняння та визначення пріоритетів. Вищий показник ризику, звичайно, вказує на вищий рівень ризику, з більш терміновими зусиллями пом’якшення.

Такі оцінки допомагають організаціям легко порівнювати ризики та визначати, як розподіляти ресурси для оптимальних стратегій реагування на ризики.

На практиці процес аналізу загрози виглядає наступним чином:

- етапи аналізу ризиків. Ідентифікація активів та їх цінності - на першому етапі слід ідентифікувати активи, які мають значення для банку, зокрема дані клієнтів, фінансові операції та критичні IT-системи. Розуміння цінності кожного активу допомагає в оцінці потенційних збитків у разі інциденту;
- аналіз загроз. Фінансове шахрайство - кібершахраї можуть здійснювати спроби отримати доступ до банківських систем для викрадення коштів чи даних клієнтів. Фішинг і соціальна інженерія - зловмисники можуть обманом отримати облікові дані користувачів і доступ до системи. DDoS-

* науковий керівник

атаки- такі атаки можуть блокувати доступ до онлайн-банкінгу, викликаючи збитки та втрату довіри клієнтів. Внутрішні загрози-включають випадкові чи навмисні дії співробітників, які можуть привести до витоку даних;

- аналіз вразливостей. Оцінка вразливостей є критичним етапом, який містить: перевірку систем на наявність відомих вразливостей, таких як відсутність актуальних оновлень чи неправильно налаштовані політики доступу. Аналіз прав доступу співробітників та моніторинг аномальної активності, що може свідчити про внутрішні загрози або шкідливу активність;
- оцінка ризиків. Оцінювання ризиків базується на врахуванні серйозності, ймовірності та виявлення ризику [3]. SIEM-системи- дають змогу моніторити мережу в реальному часі та автоматично генерувати попередження про потенційні загрози. SOAR-системи- забезпечують оркестрацію, автоматизацію та реагування на інциденти, що знижує людські помилки та підвищує швидкість реакції. Штучний інтелект і машинне навчання- використання цих технологій дає змогу банкам виявляти аномалії у великих обсягах даних, що сприяє швидшому виявленню шахрайства та інших загроз;
- відповідність регуляторним вимогам. Дотримання міжнародних та національних стандартів безпеки, зокрема PCI DSS, ISO/IEC 27001 [4], а також положення НБУ №95 [5], забезпечує виконання вимог безпеки для банківської сфери. Це передбачає обов'язковий захист даних платіжних карток та дотримання процедур, що знижують ризики інформаційної безпеки.

Висновок. Аналіз ризиків інформаційної безпеки в банківській системі є критично важливим процесом, що вимагає постійної уваги та вдосконалення. З огляду на зростаючі загрози, такі як фінансові шахрайства, фішинг, DDoS-атаки та внутрішні загрози, банки повинні впроваджувати сучасні технології для своєчасного виявлення і реагування на ці виклики. Важливою складовою цього процесу є інтеграція SIEM та SOAR-систем, які забезпечують ефективний моні-

* науковий керівник

торинг загроз та автоматизацію реагування, що, в свою чергу, допомагає зменшити кількість людських помилок. Загалом, ефективний аналіз ризиків інформаційної безпеки в банківській системі вимагає комплексного підходу, який містить технічні рішення, регуляторні вимоги та сучасні технології, забезпечуючи цілісний захист фінансових даних у контексті глобальних кіберзагроз.

Список використаних літературних джерел

[1] Потій О., Горбенко Ю., Замула О., Ісірова К. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою. // Радіотехніка. – 2021. – № 3 (206). – С. 5-24. DOI: 10.30837/rt.2021.3.206.01.

[2] Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.

[3] Карпович І. М., Гладка О. М., Бур'ян Д. Т. Сучасні технології оцінки ризиків інформаційної безпеки в електронній комерції. – Інформаційні технології та комп'ютерна інженерія. – Вінниця: ВНТУ, 2022.

[4] PCI Security Standards Council. PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. PCI DSS, 2018.

[5] Правління Національного банку України 28 вересня 2017 року прийняло постанову №95, якою затвердило Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України (далі – постанова №95). https://bank.gov.ua/ua/news/all/natsionalniy-bank-posilyuye-vimogi-do-informatsiynoyi-bezpeki-ta-kiberzahistu-v-bankah-ukrayini

[6] Американське агентство кіберзахисту https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector

[7] Державна служба спеціального зв'язку та захисту України https://cip.gov.ua/

Analysis of information security risks in the banking system

Yuriy Furdas, Svitlana Yatsyshyn

The topic is devoted to the study of modern methods and technologies for identification, assessment and management of risks in the banking sector. Given the high

* науковий керівник

level of confidentiality of financial data and the critical importance of continuity of banking operations, the banking system is one of the most vulnerable sectors to cyber attacks. The main focus of the research is on identifying the main threats, such as financial fraud, insider threats, phishing, DDoS-attacks, as well as the vulnerabilities of banks' information systems. In addition to technical aspects, regulatory requirements such as PCI DSS, which affect the security of payment transactions and require banks to adhere to high data protection standards, are also considered. The importance of automation and technology integration to reduce human error and increase incident response speed is highlighted.

* науковий керівник