УДК 004.056

А. О. Рагуліна, О. А. Боднар

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ФІНАНСОВИХ ДАНИХ: СУЧАСНІ ПІДХОДИ ТА РИЗИКИ

Миколаївський національний аграрний університет

Анотація: *У зв'язку зі стрімким розвитком інформаційних технологій та переходом до цифрової економіки, питання кібербезпеки та захисту фінансових даних набувають все більшого значення. У дослідженні проаналізовано сучасні підходи до забезпечення кібербезпеки та захисту фінансових даних, а також ідентифіковано основні ризики, які можуть виникнути в цій сфері.*

Ключові слова: цифровізація, кібербезпека, інформаційні технології, фінанси, економіка.

Abstract: *In connection with the rapid development of information technologies and the transition to a digital economy, issues of cyber security and protection of financial data are becoming increasingly important. The study analyzed modern approaches to ensuring cyber security and protecting financial data, and also identified the main risks that may arise in this area.*

Keywords: digitalization, cyber security, information technology, finance, economy.

У сучасному цифровому світі, де фінансові операції відбуваються в онлайн-режимі, кібербезпека та захист фінансових даних стають надзвичайно важливими завданнями для підприємств, корпорацій та приватних осіб. Висока вразливість цих даних перед кіберзлочинцями може призвести до серйозних фінансових втрат та порушення довіри споживачів до фінансових установ, що визначає актуальність теми дослідження.

Згідно з інформацією від компанії McAfee, яка спеціалізується на розробці антивірусного програмного забезпечення, кіберзлочинці щорічно завдають світовій економіці збитків на рівні $600 млрд. Водночас, за даними страхового концерну Lloyd's, ця цифра трохи скромніша, $400 млрд щорічно. Компанія Herjavec Group, що спеціалізується на консалтингу у сфері кібербезпеки, вказує, що наразі у світі налічується понад 6 млрд. користувачів Інтернету, проте до 2030 року ця кількість зросте до 7,5 млрд. Згідно з прогнозами Ericsson, 2023 року кількість підключених до глобальної мережі пристроїв досягнула 30 млрд., що майже вдвічі більше, ніж у 2017 році [1].

Незважаючи на використання сучасних технологій та стратегій, існують певні ризики, пов'язані з кібербезпекою та захистом фінансових даних. Деякі з найбільш поширених ризиків включають:

1. Атаки з використанням соціальної інженерії, які спрямовані на отримання конфіденційної інформації від працівників або користувачів;
2. Використання новітніх технологій кіберзлочинцями для уникнення захисних заходів та вразливостей систем;
3. DoS-атаки, прямовані на паралізацію діяльності компанії шляхом перевантаження серверів надмірним обсягом запитів, що призводить до недоступності веб-сайтів. Під час таких атак можуть страждати різні компоненти цифрової інфраструктури;
4. SQL-ін’єкції, спрямовані на використання вразливостей веб-сайтів та програмного забезпечення, яке працює з базами даних. Ця атака полягає у вставці спеціально сформованих запитів, що містять шкідливі команди, для отримання несанкціонованого доступу до конфіденційної інформації та можливості зміни структури бази даних;
5. Внутрішні загрози, коли працівники або співробітники намагаються використовувати доступ до систем для несанкціонованої діяльності або витоку даних [3].

Кіберзлочинці також можуть використовувати обманні техніки через корпоративну електронну пошту. Вони надсилають жертвам листи, які здаються відправленими від колег або партнерів з проханням оплатити рахунок. Однак, замість достовірної електронної адреси або банківського рахунку шахраї вказують свої дані, щоб отримати гроші [1].

Поява та активна популяризація серед інтернет-спільноти розмаїття видів криптографчних грошей, емісія й функціонування яких забезпечується платформами блокчейну та криптографією, а не нормативно-правовою базою держави, несе в собі як безпрецедентні можливості, так і системні

ризики. Особливе місце серед останніх займає анонімність й деперсоніфікація здійснення платежів і фінансових розрахунків. При цьому курс криптовалют не підпорядковується волі держави чи центробанку, а лише математичним розрахункам [2, с. 44].

Намагаючись запобігти кібератакам та зберегти конфіденційність фінансових даних, багато компаній та урядових установ впроваджують комплексні стратегії кібербезпеки. Ці стратегії включають в себе:

— використання сучасних технологій шифрування даних, щоб захистити їх від несанкціонованого доступу;

— розробка та впровадження надійних систем аутентифікації та авторизації, щоб забезпечити тільки дозволений доступ до фінансових даних;

— постійний моніторинг за допомогою сучасних аналітичних інструментів для виявлення підозрілих активностей та негайної реакції на них;

— організація навчання кібербезпеці персоналу з метою підвищення свідомості щодо потенційних загроз та правильного реагування на них.

У 2018 році було проведено дослідження глобальних тенденцій інформаційної безпеки. Загалом, було зроблено наступні висновки.

У заяві компанії PwC Ukraine про «Посилення цифрового середовища проти кіберзагроз» визначено, що для успішного управління кіберризиками та збереження конфіденційності необхідно побудувати вертикальну стратегію, що охоплює всі сфери підприємства, й інтегрувати концепцію стійкості у комерційну діяльність. Ця стратегія має базуватись на глибокому розумінні кіберзагроз і визначенні ключових активів, що потребують найвищого рівня захисту. Важливо також розробити цілісну концепцію оцінки прийнятного рівня ризику. Керівництво повинно сприяти розвитку культури управління кіберризиками на всіх рівнях організації, а стійкість до кіберзагроз повинна розглядатись як важливий аспект забезпечення економічної ефективності та отримання вигоди, а не просто як засіб запобігання ризикам. Наприклад, досягнення більш високого рівня стійкості до ризиків може сприяти підвищенню економічної ефективності на довгостроковій основі [5, с. 12].

Отже, важливість кібербезпеки та захисту фінансових даних у сучасному цифровому середовищі не викликає сумнівів. Запровадження комплексних стратегій кібербезпеки, таких як використання сучасних технологій шифрування, розробка міцних систем аутентифікації та авторизації, постійний моніторинг та підвищення свідомості персоналу є ключовими елементами для ефективного захисту фінансових даних. Однак існують певні ризики, такі як соціальна інженерія, використання новітніх технологій кіберзлочинцями та внутрішні загрози, які потребують постійного вдосконалення стратегій та реагування на нові виклики. Лише шляхом поєднання технологічних інновацій, ефективного управління ризиками та постійного навчання персоналу можна забезпечити надійний захист фінансових даних цифрової епохи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Харламов П. Пігулка від хакерів: як бізнес захищає себе від кібератак. *Mind*. 2019. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak. (дата звернення: 20.02.2024).

2. Кібербезпека: поради щодо захисту ваших особистих даних. *New Line Technologies*. 2023. URL: https://newline.tech/cybersecurity-recommendations-for-protecting-personal-data-uk/ (дата звернення: 21.02.2024).

3. Ризики для фінансової кібербезпеки: як компаніям з ними впоратися. *ESET*. 2021. URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/riski-dlya-finansovoy-kiberbezopasnosti-kak-kompaniyam-s-nimi-spravitsya/ (дата звернення: 20.02.2024).

4. Kovalchuk A., Stetsenko S. Financial risks in the face of digital transformation. *Public law*. 2020. No. 37. P. 43–49. URL: https://doi.org/10.37374/2020-37-04 (дата звернення: 21.02.2024).

5. Посилення цифрового середовища проти кібер-загроз. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік. *Cybersecurity and Privacy*. *PwC*. 2018. 22 с. URL: https://www.pwc.com/ua/uk/survey/2018/strengthening-digital-society-against-cyber-shocks.html (дата звернення: 21.02.2024).

Рагуліна Анастасія Олександрівна, здобувач вищої освіти обліково-фінансового факультету, Миколаївський національний аграрний університет, Миколаїв, e-mail: nastya.ragulina.2004@gmail.com

Боднар Олена Андріївна, кандидат економічних наук, доцент, доцент кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, Миколаїв e-mail: bodnaroa@mnau.edu.ua

Rahulina Anastasiia O. – graduate of the accounting and finance faculty, Mykolaiv National Agrarian University, Mykolaiv, e-mail: nastya.ragulina.2004@gmail.com

Bodnar Olena A. – PhD (Economics), Associate Professor of the Department of Finance, Banking and Insurance, Mykolayiv National Agrarian University, Mykolayiv, e-mail: bodnaroa@mnau.edu.ua