кому міжнародному рівні, визначити траєкторії подальшого професійного зростання та одразу впроваджувати нові навички й інструменти у повсякденну роботу.

Усі перелічені активності у напрямі актуалізації навчального процесу та науково-впроваджувальної діяльності є результатом постійної системної роботи всіх учасників освітнього процесу кафедри інформаційної діяльності та медіакомунікацій Інституту гуманітарних наук Національного університету «Одеська політехніка» та міжинститутської лабораторії обчислювальної техніки та мережевих технологій iXTF Labs. Попереду безліч нових інновацій, проєктів та творчих впроваджень.

Список використаних джерел

1. Захаревич М., Жмуд О. Цифрові платформи для проєктної діяльності у вищій освіті: шлях до формування компетентностей XXI століття. *Педагогічні науки: теорія, історія, інноваційні технології.* 2025. № 2(142). С. 292–304.

2. Manifesto for Agile Software Development / K. Beck, M. Beedle, A. van Bennekum et al. URL: https://agilemanifesto.org/ (дата звернення: 25.05.2026).

3. Schwaber K., Sutherland J. The Scrum Guide. URL: https://scrumguides.org/scrum-guide.html (дата звернення: 25.05.2026).

4. Vacanti D., Coleman J. The Kanban Guide. URL: https://kanbanguides.org/english/ (дата звернення: 25.05.2026).

УДК 002.6:004.056:005.334:336.71

Ірина Тюрменко, д-р іст. наук, професор,
Сергій Горєв, здобувач ОС «Магістр»
Національний університет «Київський авіаційний інститут», м. Київ

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКИХ УСТАНОВАХ

Анотація. Досліджено особливості управління ризиками інформаційної безпеки в банківських установах в умовах цифровізації фінансового сектору. Розглянуто основні кіберзагрози, що впливають на діяльність банків, зокрема несанкціонований доступ до інформаційних систем, фішингові атаки, DDoS-атаки та ризики, пов'язані з людським фактором. Проаналізовано основні етапи процесу управління ризиками інформаційної безпеки, а також технічні та організаційні заходи щодо їх мінімізації. Окрему увагу приділено діяльності Національного банку України у сфері кіберзахисту, роботі команди реагування на кіберінциденти CSIRT-NBU та інформаційно-просвітницьким проєктам #КіберКіт і #КіберПес.

Ключові слова: банківські установи, управління ризиками, кіберзагрози, інформаційна безпека, кібербезпека, захист інформації.

У сучасних умовах цифрової трансформації фінансового сектору питання забезпечення інформаційної безпеки набуває особливої актуальності для банківських установ. Банки здійснюють щоденну обробку величезних обсягів фінансової інформації, персональних даних клієнтів, платіжних документів та інших конфіденційних відомостей, що робить їх одними з найпривабливіших об'єктів для кіберзлочинців. Розвиток онлайн-банкінгу, мобільних додатків, безконтактних платежів та дистанційного обслуговування клієнтів значно підвищив ефективність фінансових послуг, проте одночасно збільшив кількість потенційних загроз інформаційній безпеці. У зв'язку з цим управління ризиками інформаційної безпеки стає стратегічним напрямом діяльності кожної банківської установи та необхідною умовою її стабільного функціонування.

Управління ризиками інформаційної безпеки – це комплексний процес виявлення, оцінювання, контролю та мінімізації загроз, які можуть вплинути на конфіденційність, цілісність і доступність інформаційних ресурсів банку. Основною метою такого управління є забезпечення захисту інформаційних активів та безперервності банківської діяльності навіть за умов реалізації кіберзагроз або технічних збоїв. Втрата контролю над інформаційними ресурсами може призвести як до прямих фінансових збитків, так і до втрати конкурентних переваг на ринку фінансових послуг [2].

Сучасні банки стикаються з великою кількістю ризиків інформаційної безпеки. Одним із них є несанкціонований доступ до інформаційних систем. Для цього зловмисники використовують шкідливе програмне забезпечення, фішингові повідомлення, соціальну інженерію та інші інструменти кіберзлочинності. Особливу небезпеку становлять цільові атаки на банківські установи, під час яких злочинці можуть тривалий час залишатися непоміченими, поступово отримуючи доступ до конфіденційних даних або фінансових ресурсів.

Людський фактор також складає небезпечну групу ризиків. Працівники можуть випадково розголосити конфіденційну інформацію, використовувати ненадійні паролі, відкривати шкідливі вкладення в електронних листах або порушувати встановлені правила роботи з інформаційними ресурсами. Існує ризик навмисних дій працівників, які можуть використовувати банківську інформацію у власних інтересах або на користь третіх осіб.

Кібератаки становлять чи не основну загрозу для банківської системи. Найбільш поширеними серед них є DDoS-атаки, які перевантажують сервери, порушуючи доступ до банківських послуг. Такі атаки можуть призвести до тимчасового блокування роботи мобільного додатка або вебпорталу банку, що впливає на рівень довіри клієнтів. Не менш небезпечними є атаки із застосуванням програм-вимагачів, які шифрують інформацію та вимагають викуп за відновлення

доступу до неї. Подібні інциденти можуть мати катастрофічні наслідки через втрату доступу до даних та операційних систем.

В умовах воєнного стану кількість кібератак на фінансовий сектор України продовжує зростати, що підтверджується дослідженнями щодо функціонування банків в умовах воєнних ризиків та кіберзагроз [1]. Процес управління ризиками інформаційної безпеки розпочинається з ідентифікації активів. До них належать бази даних клієнтів, серверне обладнання, програмне забезпечення, платіжні системи, внутрішня документація, електронні архіви та канали зв'язку. Після визначення активів здійснюється аналіз потенційних загроз. На основі отриманих результатів формується перелік ризиків, які потребують оцінювання.

Оцінка ризиків дає змогу визначити ймовірність виникнення конкретної загрози та масштаб її можливих наслідків. Для цього застосовуються такі аналітичні методи, як матриці ризиків, експертні оцінки, сценарний аналіз та кількісні методики розрахунку потенційних збитків. За результатами оцінювання визначаються ризики, які потребують невідкладного розв'язання [4].

Одним із ключових напрямів управління ризиками є впровадження технічних засобів інформаційної безпеки. До них належать міжмережеві екрани, системи виявлення та запобігання вторгненням, антивірусний захист, засоби шифрування даних, системи резервного копіювання та багатофакторна автентифікація користувачів. Використання таких технологій сприяє суттєвому зниженню ймовірності успішного здійснення кібератак та мінімізуванню можливих наслідків інцидентів [3].

Організаційний напрям діяльності банків спрямований на розроблення внутрішньої політики інформаційної безпеки, регламенти роботи з конфіденційною інформацією, процедури реагування на інциденти та плани забезпечення безперервності діяльності. Регулярно проводяться аудити інформаційної безпеки, тестування на проникнення та перевірки відповідності вимогам міжнародних стандартів, зокрема ISO/IEC 27001. Особлива увага приділяється підготовці персоналу, оскільки підвищення рівня обізнаності працівників дає можливість значно зменшити ризики, пов'язані з людським фактором.

Суттєву роль у забезпеченні інформаційної безпеки банківського сектору відіграє Національний банк України (далі – НБУ), який встановлює нормативні вимоги щодо організації систем управління інформаційною безпекою та кіберзахистом [4]. Банки зобов'язані впроваджувати комплексні системи управління ризиками, здійснювати моніторинг кіберзагроз та повідомляти регулятора про серйозні інциденти інформаційної безпеки. Водночас в Україні функціонує спеціалізована команда реагування на кіберінциденти у фінансовому секторі, яка координує дії банків під час виникнення масштабних кіберзагроз та сприяє обміну інформа-

цією щодо нових методів атак [5]. Важливим напрямом підвищення рівня кіберграмотності є інформаційно-просвітницькі проєкти НБУ #КіберКіт та #КіберПес, реалізовані в межах кампанії «КібербезпекаФінансів» [5; 6]. Метою цих проєктів є формування навичок безпечної поведінки в цифровому середовищі, розпізнавання шахрайських схем та захисту персональних даних під час використання банківських сервісів.

Отже, управління ризиками інформаційної безпеки є одним із найважливіших напрямів діяльності банківських установ в умовах цифрової економіки. Ефективна система управління ризиками дає змогу своєчасно виявляти загрози, мінімізувати можливі збитки, забезпечувати безперервність надання банківських послуг та підтримувати високий рівень довіри клієнтів. З огляду на постійне зростання кількості кіберзагроз і вдосконалення методів кіберзлочинців, банки повинні безперервно розвивати власні системи інформаційної безпеки, поєднуючи сучасні технологічні рішення, ефективні організаційні механізми та високий рівень підготовки персоналу. Це сприятиме забезпеченню стійкості банківської системи та надійному захисту фінансових ресурсів і даних клієнтів.

Список використаних джерел

1. Апацький В. В. Українські банки в умовах воєнних ризиків, кіберзагроз та невизначеності. *Журнал стратегічних економічних досліджень.* 2026. № 2(3). URL: https://jrnl.knutd.edu.ua/index.php/jseconres/article/view/2041 (дата звернення: 11.06.2026).

2. КібербезпекаФінансів: освітня кампанія Національного банку України та Держспецзв'язку. URL: https://promo.bank.gov.ua/payment-security/ (дата звернення: 10.06.2026).

3. Актуалізовано підходи до управління ризиками в банках і банківських групах. *Офіційний вебсайт Національного банку України.* URL: https://bank.gov.ua/ua/news/all/aktualizovano-pidhodi-do-upravlinnya-rizikami-v-bankah-bankivskih-grupah (дата звернення: 10.06.2026).

4. Контроль за кіберзахистом та інформаційною безпекою банків посилюється. *Офіційний вебсайт Національного банку України.* URL: https://bank.gov.ua/ua/news/all/kontrol-za-kiberzahistom-ta-informatsiynoyu-bezpekoybankiv-posilyuyetsya (дата звернення: 10.06.2026).

5. Національний банк посилює вимоги до інформаційної безпеки та кіберзахисту в банках України. *Офіційний вебсайт Національного банку України.* URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-posilyuye-vimogi-do-informatsiynoyi-bezpeki-ta-kiberzahistu-v-bankah-ukrayini (дата звернення: 12.06.2026).

6. Команда реагування на кіберінциденти в банківській системі України (CSIRT-NBU). *Центр кіберзахисту Національного банку України.* URL: https://cyber.bank.gov.ua/ (дата звернення: 15.06.2026).