

DOI <https://doi.org/10.30525/978-9934-26-277-7-26>

## DIGITAL SERVICES OF BANKS IN THE ASPECT OF MODERN THREATS

### ДІДЖИТАЛ-СЕРВІСИ БАНКІВ У АСПЕКТИ СУЧАСНИХ ЗАГРОЗ

**Boldov A. O.**  
*Graduate Student  
State Research Institute  
of Informatization and Modeling  
of the Economy  
Kyiv, Ukraine*

**Болдов А. О.**  
*аспірант  
Державний науково-дослідний  
інститут інформатизації  
та моделювання економіки  
м. Київ, Україна*

У час розвитку цифрових технологій практично вже всі сервіси у діяльності банків виражені як онлайн-послуга, таким чином відбувається повна діджиталізація банківського сектору [1].

Діджитал-сервіси банків стають все більш удосконаленими для легкого використання за допомогою телефона чи планшета. Але основною перевагою діджитал-сервісів – це зручність не лише для клієнта а і для працівників та співробітників банківських установ. Діджиталізація дає змогу зберігати та обробляти величезні об'єми цифрових даних. Але, як правило, це приватна інформація та індивідуально-особисті дані то виникає морально-етична потреба у конфіденційності.

Тому актуалізується те, що діджиталізація має ряд загроз та небезпек, а саме: несанкціонованого доступу до інформації, «зливу» персональних даних, їх зміна для подальшого негативного або корупційного ефекту чи просто знищення.

Безпека і захист інформації та персональних даних стає ще однією вагомою проблемою банківської установи. Головне завдання тепер є передувати, уникати та боротися із кіберзлочинами, а саме утримання величезних масивів даних, які повинні зберігатися з гарантуванням конфіденційності та безпеки їх потрапляння у «другі руки».

Захист баз даних є одним із складних завдань бо кожна з них потребує індивідуального підходу до організації захисту та безпеки і включає велику кількість технологій та інструментів.

Найбільш ефективними заходами є:

- шифрування файлів та резервних копій баз даних;
- своєчасне оновлення програмного забезпечення;
- здійснення контролю безпеки доступу до бази даних;
- аудит та моніторинг активності бази даних [2].

Вищеописані заходи є найбільш популярними і дозволяють уникнути хакерських атак на банківські сервери. Для банку – це його імідж, для клієнта – це і конфіденційність інформації та особистих даних, і запобігання втрати персональної інформації, і достатній рівень довіри до нових технологій

Діджитал-сервіси банку також відмінні за своєю системою шифрування даних що дозволило створити систему безконтактних платежів [1]. Цей процес носить назву токенизація і банки отримують не самі персональні дані, а їх цифровий формат у вигляді токена. Таким чином, конфіденційна інформація не потрапляє до чужих рук.

Токенизація є стандартною процедурою. Але її ефективність зростає в разі при створенні резервних копій даних яке захищає від хакерських атак і від технічних збоїв обладнання та програмним забезпеченням. Також варто зазначити що така інформація має міститися на серверах не зв'язаних із «світом», а саме не взаємодіяти безпосередньо через інтернет, не міститися в «хмарах» і на зовнішніх хостингах [4].

На разі, варто ще зупинити увагу на такому аспекті як безпечний доступ до даних. Тут варто використовувати автоматизоване керування яке полягає у наданні дозвілу за допомогою груп та розмежування ролей, а не надання прямого доступу. Його переваги у наступному:

- надання тимчасового паролю, який буде генеруватиметься при кожному вході до бази даних;
- відстеження дій виконаних конкретним користувачем;
- підбір для використання надійних паролей (містить одночасно символи, цифри, літери (у тому числі великі)) [4].

Отже, кібербезпека банку, при використанні ним у операційній діяльності діджитал-сервісів, є сучасною і вагомим проблемою, оскільки захист персональної інформації та фінансових даних є очевидним. Запобігання витоку інформації потребує системного вивчення та комплексного підходу і виконання таких завдань має бути покладене на фахівців відповідного рівня.

Це є не тільки запитом сучасного цифрового суспільства а і перспектива у області фінансових технологій для реалізації стратегій подальшого розвитку діджитал-сетрісів банківської сфери.

Всі ці заходи необхідні для мінімізації ризиків, пов'язаних з втратою конфіденційної інформації баз даних і захисту інформаційної системи. *Використання новітніх технологій та підходів носить глобальний характер і захист від сучасних загроз потребують все більшого наукового вивчення.*

### **Література:**

1. Андрушків І. П., Надієвець Л. М. Діджиталізація в банківському секторі : світовий та вітчизняний досвід. *Проблеми економіки*. 2018. № 4. С. 195– 200. URL: [http://nbuv.gov.ua/UJRN/Pecon\\_2018\\_4\\_24](http://nbuv.gov.ua/UJRN/Pecon_2018_4_24) (дата звернення: 12.12.2020 р.).

2. Болдова А. Електронні фінансові послуги. / Антоніна Болдова, Юлія Болдова // *Dynamics of the development of world science*. Abstracts of the 6th International scientific and practical conference. Perfect Publishing. Vancouver, Canada. 2020. P. 377–381. URL: <http://sci-conf.com.ua>

3. Корнєєв В. В., Вергелюк Ю. Ю., Ганцяк М. О. Боргові ринки в умовах нециклічних викликів. *Інноваційні стратегії та моделі економічних трансформацій в умовах євроінтеграційних викликів* : матер. міжнар. наук.- практ. Internet-конф., 15 травня 2020 р. Харків – Ужгород – Софія – Пшеворськ. Софія, 2020. С. 88–90.

4. Логінова Н. І. Безпека баз даних. *Кібербезпека в сучасному світі* : матеріали III Всеукраїнської наук.-практ. конф., (м. Одеса, 19 листопада 2021 р.). Одеса, 2020. 148 с. DOI 10.32837/11300.15973