

3. Державна податкова служба України. Роз'яснення щодо спрощеної системи оподаткування для аграрного сектору. URL: https://tax.gov.ua/data/material/000/044/51180/1Podatkova_deklarats_ya_platnika_dinogo_podatku_chetverto_grupi.pdf.
4. Інститут аграрної економіки. Аналітичний звіт про ефективність податкової політики в аграрному секторі. URL: <http://www.iae.org.ua/>.
5. Європейський банк реконструкції та розвитку. Оцінка системи оподаткування сільського господарства в Україні. URL: <https://mof.gov.ua/uk/ebrr>.
6. Світовий банк. Дослідження про податкові режими в аграрному секторі країн, що розвиваються. URL: <https://documents1.worldbank.org/curated/en/306091468129288953/pdf/449840UKRAINIA1aineFINAL0Box334133B.pdf>.
7. OECD. Taxation in Agriculture: International Practices and Recommendations. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/02/taxation-in-agriculture_cc3f80fa/073bdf99-en.pdf.
8. Європейська комісія. Політика оподаткування аграрного сектору в країнах ЄС. URL: https://niss.gov.ua/sites/default/files/2011-07/agro_polytyka-f29c7.pdf.

***Annotation:** The main taxes affecting the activities of agricultural enterprises, in particular the single tax of the fourth group and VAT, are analyzed. The advantages and disadvantages of their use by agricultural enterprises that apply the simplified taxation system are considered. The author emphasizes the improvement of control mechanisms for simplified taxation through electronic monitoring and increasing the level of transparency of tax reporting. The international experience of applying special tax regimes for the agricultural sector is considered. In order to support Ukrainian agricultural enterprises, preferential taxation is advisable, which will increase their competitiveness in the international market.*

***Keywords:** tax system, agrarian sector, tax privileges, single tax, VAT, state support.*

Науковий керівник:

Бурковська А. В.

канд. екон. наук, доцентка,

доцентка кафедри фінансів, банківської справи та страхування

Миколаївський національний аграрний університет

УДК 004.9.056.53:336.71

Цифровізація як важливий елемент ефективного банківського менеджменту в контексті запобігання кібератакам

Тетяна Нестерчук,

здобувачка вищої освіти спеціальності D2 Фінанси, банківська справа, страхування та фондовий ринок

Миколаївський національний аграрний університет

м. Миколаїв, Україна

Анотація: розглянуто роль цифровізації в банківському менеджменті, зокрема вплив технологій на ефективність фінансових послуг та оптимізацію процесів. Виявлено, що зростання цифровізації створює нові виклики в кібербезпеці, вимагаючи удосконалення методів захисту та управління кіберризиками. З'ясовано, що для забезпечення кібербезпеки банку та ефективності його діяльності важливо впроваджувати новітні технології та підвищувати обізнаність працівників і клієнтів.

Ключові слова: цифровізація, банківський менеджмент, кібербезпека, захист даних.

Цифровізація є фундаментальним чинником ефективного банківського менеджменту, оскільки сприяє підвищенню якості фінансових послуг, оптимізації операційних процесів, удосконаленню управління ризиками та забезпеченню конкурентоспроможності, фінансової та інформаційної безпеки банку, оскільки допомагає виявляти шахрайські операції, ефективніше аналізувати поведінку клієнтів та прогнозувати потенційні ризики.

Під «цифровізацією» розуміють трансформацію економічних відносин та бізнес-моделей, що включає перехід до цифрового бізнесу, зміну підходів до взаємодії суб'єктів ринку та впровадження нових технологій; вона відкриває додаткові можливості для отримання прибутку, створення цінності, оптимізації управління виробництвом послуг, а також сприяє вирішенню актуальних економічних проблем на рівні окремих галузей та компаній [1].

Інтеграція штучного інтелекту (ШІ), хмарних технологій, блокчейну та біометричної аутентифікації відіграє ключову роль у цифровій трансформації банківського сектору, дозволяючи автоматизувати основні процеси, оптимізувати управління ресурсами, знижувати операційні витрати та підвищувати рівень безпеки. ШІ та технології машинного навчання сприяють покращенню аналізу великих масивів даних, що дає змогу банкам глибше розуміти поведінку клієнтів, прогнозувати їхні фінансові потреби та пропонувати персоналізовані послуги. Завдяки автоматизованим алгоритмам кредитний скоринг стає більш точним і швидким, що дозволяє ефективніше оцінювати кредитоспроможність позичальників, мінімізувати ризики дефолтів і водночас розширювати доступ до фінансування. Хмарні технології забезпечують гнучкість у зберіганні та обробці даних, підвищують ефективність внутрішніх процесів і сприяють безперебійному доступу до фінансових сервісів як для клієнтів, так і для банківських працівників. Вони дозволяють скоротити витрати на підтримку ІТ-інфраструктури та прискорюють впровадження нових цифрових продуктів. Блокчейн-технології сприяють підвищенню прозорості та безпеки фінансових операцій завдяки розподіленій природі реєстрів і незмінності даних. Це особливо важливо для запобігання фінансовим шахрайствам, вдосконалення міжбанківських розрахунків і розробки смарт-контрактів, які автоматизують виконання угод за визначеними умовами. Біометрична аутентифікація підвищує рівень безпеки

доступу до банківських послуг, зменшуючи ризик шахрайства та несанкціонованого доступу до рахунків. Використання відбитків пальців, розпізнавання обличчя або голосової ідентифікації робить банківські операції не лише більш захищеними, а й зручними для клієнтів [2].

Проте із зростанням рівня цифровізації загострюється питання кібербезпеки. Зростання ролі ІІІ у кіберзлочинності створює нові виклики для фінансових установ. Зловмисники використовують deepfake та синтетичне шахрайство для обходу традиційних систем захисту. У 2023 р. збитки від deepfake-атак сягнули 12,3 млрд дол. США, а до 2027 р. прогнозується їх зростання до 40 мільярдів [3]. Банки через володіння великими обсягами конфіденційної інформації та фінансових ресурсів є головною мішенню для таких атак, що вимагає вдосконалення механізмів захисту та управління кіберризиками [3].

Зважаючи на високі вимоги до збереження конфіденційності, банки зобов'язані впроваджувати ефективні методи менеджменту для захисту від кіберзагроз. Ключовими напрямками є освітні ініціативи, стратегії протидії кіберзлочинності, використання новітніх технологій (ІІІ) та інтеграція сучасних систем захисту даних. Основними напрямками боротьби з кіберзлочинністю є постійний моніторинг загроз, виявлення вторгнень, співпраця з регуляторами і міжнародними організаціями, застосування технологій машинного навчання для виявлення аномалій та попередження атак [4]. ІІІ і машинне навчання допомагають банкам не лише швидше виявляти кіберзагрози, але й прогнозувати їх. Завдяки використанню алгоритмів, що аналізують поведінку злочинців, банки можуть передбачити й запобігти можливим атакам до їхнього здійснення. Це значно підвищує ефективність заходів безпеки і зменшує ризики для банків. Однак технології ІІІ потребують постійного вдосконалення, оскільки зловмисники також адаптуються до нових методів захисту [4]. Особливо важливим аспектом забезпечення кібербезпеки банком є підвищення рівня обізнаності працівників і клієнтів банків щодо потенційних кіберзагроз. Банки активно реалізують освітні програми, зокрема через тренінги, семінари, вебінари та онлайн-курси з кібербезпеки, що дозволяють персоналу своєчасно розпізнавати загрози, такі як фішинг, соціальна інженерія та зловмисні програми. Це дозволяє оперативно реагувати на інциденти та запобігати великим фінансовим втратам. Зокрема, клієнтам надаються рекомендації щодо безпеки використання онлайн-банкінгу, методів захисту особистих даних, складних паролів та двофакторної автентифікації, що значно знижує ризик злому акаунтів [4].

Важливим елементом є і захист персональних даних клієнтів. Для цього банки використовують сучасні технології шифрування, які забезпечують конфіденційність даних, що передаються через мережі, а також багаторівневу автентифікацію для ускладнення несанкціонованого доступу. Впровадження таких технологій знижує ймовірність викрадення даних та забезпечує високу ступінь захисту під час здійснення фінансових операцій. Завдяки комплексному підходу використання технологій шифрування, систем моніторингу та освітніх

програм для клієнтів банки можуть значно підвищити рівень безпеки і знижувати ризики кіберзлочинності [4].

Отже, цифровізація сприяє підвищенню ефективності, зниженню витрат та забезпеченню високої конкурентоспроможності банківських установ і потребує кібербезпеки. Управління кіберризиками, інтеграція ІІІ в процеси безпеки та постійне вдосконалення методів захисту є необхідними кроками для мінімізації ризиків і забезпечення безпеки. Тому для банків важливо активно інвестувати в новітні технології, удосконалювати внутрішні процеси та надавати клієнтам необхідні інструменти для захисту їхніх особистих даних, що дозволяє знижувати ризики шахрайства та кіберзлочинності.

Список використаних джерел:

1. Береславська О.І. Трансформація банківських послуг в умовах цифровізації. *Економіка та суспільство*. 2024. Вип. 60. DOI: <https://doi.org/10.32782/2524-0072/2024-60-99>.
2. Береславська О. І., Вергелюк Ю. Ю. Новітні фінансові технології у банківській діяльності. *Researchgate*. 2024. URL: <https://salolj/369CE30>.
3. Захист ІІІ кордону: захист корпоративних систем від загроз ІІІ. *Oksim*. 2024. URL: <https://salolj/3E04890>.
4. Скорик Ю. Як банки протидіють кіберзлочинності у цифрову епоху. *Finway*. 2025. URL: <https://salolj/22454ed>.

Abstract: *The role of digitalization in banking management is considered, in particular the impact of technology on the efficiency of financial services and process optimization. It is found that the growth of digitalization creates new challenges in cybersecurity, requiring improvements in methods of protection and management of cyber risks. It is found that to ensure the cybersecurity of the bank and the efficiency of its activities, it is important to implement the latest technologies and increase the awareness of employees and customers.*

Key words: *digitalization, banking management, cybersecurity, data protection.*

Науковий керівник:

Бурковська А.В.,

канд. екон. наук, доцентка,

доцентка кафедри фінансів, банківської справи та страхування

Миколаївський національний аграрний університет

УДК 336.22

Зміни для діяльності резидентів Дія Сіті в Україні

Ангеліна Орешко,

здобувачка вищої освіти спеціальності 071 Облік і оподаткування

Миколаївський національний аграрний університет

м. Миколаїв, Україна