УДК 004.9

М.Ю. Кривов`язюк
О.П. Войтович

ОСОБЛИВОСТІ БАНКІВСЬКОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ ТА СТАНДАРТИ АУДИТУ

Вінницький національний технічний університет

Анотація.
Ця робота розглядає тему банківської інфраструктури та стандартів аудиту в Україні. Було проведено аналіз міжнародних стандартів інформаційної безпеки, таких як COBIT 2019, ISO 27001 та NIST CSF, які є важливими інструментами для забезпечення надійності фінансових установ. Дослідження спрямоване на оцінку відповідності банківських процесів сучасним вимогам безпеки та аудиту, що дозволяє підвищити стійкість фінансової системи та зменшити ризики кіберзагроз. Інтеграція цих стандартів сприяє ефективному управлінню ризиками та захисту банківських даних.
Ключові слова*: банківська інфраструктура, стандарти аудиту інформаційної безпеки, кібербезпека, ISO 27001, COBIT 2019, NIST CSF.*

Abstract.
This paper examines the banking infrastructure and audit standards in Ukraine. An analysis of international information security standards, such as COBIT 2019, ISO 27001, and NIST CSF, has been conducted, as these are essential tools for ensuring the reliability of financial institutions. The study focuses on assessing the compliance of banking processes with modern security and audit requirements, which enhances the stability of the financial system and reduces cyber threat risks. The integration of these standards contributes to effective risk management and the protection of banking data.
Keywords*: banking infrastructure, audit standards of information security,cyber security, ISO 27001, COBIT 2019, NIST CSF.*

Вступ

Сучасна банківська інфраструктура України є основою фінансової стабільності країни та потребує ефективного управління інформаційною безпекою. В умовах цифровізації банківських послуг та зростання кіберзагроз особливо важливим стає дотримання міжнародних стандартів аудиту та кіберзахисту. Впровадження таких стандартів, як COBIT 2019 [1], ISO 27001 [2] та NIST CSF [3], забезпечує надійність фінансових операцій, відповідність регуляторним вимогам і підвищує конкурентоспроможність банківських установ. У цьому дослідженні розглядаються особливості банківської інфраструктури України, нормативні вимоги та роль міжнародних стандартів у забезпеченні її ефективності.

Основна частина

Банківська інфраструктура є ключовим елементом фінансової системи України, а її ефективне функціонування залежить від впровадження сучасних стандартів аудиту та інформаційної безпеки. В умовах цифровізації банківських послуг та зростання кіберзагроз особливо актуальним стає питання забезпечення надійності та стійкості фінансових установ. З огляду на вимоги сектору Національного банку України (НБУ) та міжнародних регуляторів, імплементація міжнародних стандартів управління IT та кібербезпеки є необхідною умовою для підтримки стабільності банківського фонду.

Розвиток фінансових технологій вимагає постійного вдосконалення банківської інфраструктури та адаптації до нових загроз. Таким чином, впровадження зазначених стандартів стає не лише недостатністю, а й конкурентною перевагою. Подальші дослідження можуть бути спрямовані на оцінку ефективності їх інтеграції в банківських установах України, аналіз витрат на їх реалізацію та визначення оптимальних стратегій відповідності міжнародним вимогам.

Метою дослідження є аналіз банківської інфраструктури України, її нормативного регулювання, а також порівняння міжнародних стандартів аудиту інформаційної безпеки для підвищення ефективності та відповідності банківського сектору сучасним викликам.

Для досягнення поставленої мети було застосовано такі методи дослідження:

– Аналіз нормативно-правової бази НБУ (Постанови №88, №75, №64, №55, №30 та ін.);
– Порівняльний аналіз міжнародних стандартів COBIT 2019, ISO 27001 та NIST CSF;
– Оцінка відповідності банківських процесів вимогам ISO, NIST та НБУ.

Банківська інфраструктура України включає такі основні елементи: Національний банк України (НБУ), Систему електронних платежів (СЕП), Фонд гарантування вкладів фізичних осіб (ФГВФО), міжнародні платіжні системи та механізми фінансового моніторингу.

Регулювання аудиту здійснюється через постанови НБУ, міжнародні стандарти аудиту (ISA) та фінансової звітності (IFRS), а також базельські принципи банківського нагляду (Базель II, Базель III).

Результати порівняння міжнародних стандартів аудиту інформаційної безпеки показано в табл. 1.

COBIT 2019, ISO 27001 та NIST Cybersecurity Framework (CSF) є ключовими стандартами в банківському аудиті, але їх застосування залежить від цілей перевірки.

COBIT 2019 забезпечує комплексне управління IT та допомагає банкам відповідати стратегічним бізнес-цілям. Його варто використовувати для аудиту ефективності управління IT-процесами та відповідності регуляторним вимогам.

ISO 27001 є міжнародним стандартом інформаційної безпеки, що дозволяє банкам отримати сертифікацію та відповідати вимогам НБУ, GDPR та PCI DSS. Підходить для оцінки ризиків та впровадження політик безпеки.

NIST CSF використовується для аналізу кіберзагроз, побудови системи захисту від атак та реагування на інциденти. Він ефективний для внутрішнього аудиту банківської кібербезпеки та управління ризиками.

Таблиця 1 – Результати порівняння стандартів з аудиту інформаційної безпеки.

Критерій	COBIT 2019	ISO 27001	NIST CSF
Основне призначення	Управління IT-процесами та відповідність бізнес-цілям	Інформаційна безпека та сертифікація	Кібербезпека та управління ризиками
Область застосування	Управління IT, ефективність аудиту	Захист даних, контроль доступу	Аналіз кіберзагроз, управління інцидентами
Регуляторні вимоги	Відповідність законодавчим та нормативним актам	Вимоги НБУ, GDPR, PCI DSS	Вимоги для кібербезпеки в критичних системах
Основні принципи	Управління IT, контроль процесів	Оцінка ризиків, впровадження заходів безпеки	ідентифікація, захист, реагування
Методологія оцінки	Оцінка зрілості процесів IT	Впровадження ISMS (Система управління інформаційною безпекою)	Оцінка ризиків, контроль загроз
Підходи до аудиту	Комплексна оцінка ефективності IT	Сертифікаційний аудит	Самооцінка та адаптація до загроз
Галузі застосування	Фінансовий сектор, державне управління, корпорації	Банки, IT-компанії, організації з обробки даних	Критична інфраструктура, фінансовий сектор
Переваги	Дозволяє оцінити ефективність управління IT	Глобальне визнання, сертифікація безпеки	Гнучкість, адаптація до сучасних кіберзагроз
Недоліки	Висока складність впровадження	Дороговартісна сертифікація	Відсутність офіційної сертифікації

Важливо відзначити, що кожен банківський процес потребує відповідності певним стандартам. Основні вимоги встановлює НБУ та ISO 27001, які охоплюють управління ризиками, безпеку даних та контроль доступу. Проте, залежно від специфіки діяльності, можуть застосовуватися і більш спеціалізовані стандарти, такі як PCI DSS для обробки платежів, SOC 2 для оцінки контролів безпеки, а також ISO 22301 для забезпечення безперервності бізнесу. Хоча такі стандарти використовуються рідше, їх імплементація є обов'язковою для забезпечення повної відповідності вимогам регуляторів та підвищення надійності банківських процесів. Подальші дослідження можуть бути спрямовані на оцінку практичних аспектів імплементації цих стандартів у банківських установах України, зокрема, аналіз

ефективності їх застосування у великих та середніх банках, а також розробку рекомендацій щодо їх гармонізації з національними регуляторними вимогами.

Висновки

Аналіз банківської інфраструктури України показав, що сучасні міжнародні стандарти аудиту та кібербезпеки є ключовими для стабільності фінансового сектору. COBIT 2019 сприяє ефективному управлінню IT, ISO 27001 гарантує відповідність вимогам інформаційної безпеки, а NIST CSF дозволяє оцінювати та мінімізувати кіберризики. Інтеграція цих стандартів дозволяє банкам відповідати регуляторним вимогам та забезпечувати високий рівень безпеки фінансових операцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

ISO/IEC 27001:2013. Інформаційні технології — Методи безпеки — Системи управління інформаційною безпекою — Вимоги.

Концепція COBIT 2019: цілі управління та управління. ISACA, 2019.

Концепція кібербезпеки Національного інституту стандартів і технологій (NIST), 2018 р.

Постанова НБУ №88 "Про затвердження Положення про організацію захисту інформації в банківській системі України".

Базельський комітет з банківського нагляду. Базель II: Міжнародна конвергенція вимірювання капіталу та стандартів капіталу. Банк міжнародних розрахунків, 2004.

Базельський комітет з банківського нагляду. Базель III: Регуляторні рамки для посилення стійкості банків та банківських систем. Банк міжнародних розрахунків, 2011.

ISO/IEC 22301:2019. Безпека та стійкість — Системи управління безперервністю бізнесу — Вимоги.

PCI DSS v4.0. Стандарт безпеки даних платіжних карток. Рада стандартів безпеки PCI, 2022 р.

Інститут управління IT. «Цілі IT-контролю для Сарбейнса-Окслі: роль IT у розробці та впровадженні внутрішнього контролю над фінансовою звітністю», 2006 р.

Сміт М. «Кібербезпека в банківській справі: управління ризиками та відповідність вимогам», Wiley, 2021.

Кривов`язюк Максим Юрійович – студент групи 1БС-24м, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця. Електронна адреса: kryvovyazykmaks@gmail.com.

Kryvovyazyk Maxim Yu. – student 1BS-24m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kryvovyazykmaks@gmail.com

Науковий керівник: Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk@vntu.edu.ua

Supervisor: Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical

.