DOI: https://doi.org/10.32782/2519-884X-2024-53-12
УДК 336.71:004.056

Мельник О. В., *здобувач третього (освітньо-наукового) рівня вищої освіти*
Таврійський державний агротехнологічний університет
імені Дмитра Моторного
alexreetwell@gmail.com
ORCID: 0009-0005-3990-6920

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ НА ЗАСАДАХ МЕТАПРОСТОРУ FINTECH-ПОСЛУГ

Анотація. *В статті досліджуються процеси забезпечення безпеки банківської безпеки на засадах метапростору FinTech-послуг. Представлено методичний підхід щодо забезпечення безпеки банківської системи за регуляторними стабілізаторами СЕП НБУ, які на засадах метапростору FinTech-послуг нівелюють загрози платіжних систем в банківському інформаційному просторі, стабілізують захист учасників та користувачів платіжного портфеля банківських установ від дезінформації та шахрайства. Запропоновано синергетичну модель безпеки СЕП НБУ, із врахування сек'юритизації платіжного портфеля банківських установ на фінансовому ринку для попередження загроз та забезпечення потреб учасників та користувачів в банківському обслуговуванні. Рекомендовано критерії рівня безпеки СЕП НБУ.*

Ключові слова*: безпека, банківська система, метапростір, FinTech-послуги, система електронних платежів, платіжних портфель, платіжні системи.*

JEL code classification: G21, G24, H56

Постановка проблеми. В умовах загострення загроз повномасштабної агресії проти України терористично налаштованої рф, актуалізується проблема захисту національних інтересів, зокрема захисту банківської системи, яка втручається в усі сектори економіки, обслуговує безготівкові розрахунки, здійснює зберігання коштів та кредитне обслуговування клієнтів через національні та валютні потоки. Банківський система України, залежна від зовнішніх регуляторних механізмів захисту національної грошової одиниці, капіталізації та розподілу фінансового капіталу на електронних платіжних носіях, яким характерний високий рівень кібератак та загроз шахрайства. За відсутності захисних інформаційних ресурсів це може спричинити втрату фінансових потоків при обслуговуванні користувачів у платіжному ландшафті банківських установ, і, відповідно, докорінно дестабілізувати фінансову систему державі в цілому.

Небезпека в банківській системі суб'єктивно зумовлена фінансовими загрозами, які часто проявляються як спроба злочинців або шахраїв знищити платіжні системи та присвоїти фінансові ресурси за допомогою дій, яким надається вигляд легальних та (або) економічно обґрунтованих. В платіжних системах банківських послуг існує конфлікт інтересів, який маскується у вигляді оптимізації інформаційних носіїв для прискорення потоку фінансових ресурсів через електронні платежі. Тому миттєвий захист платіжних операцій в мережі банківської системи є результатом своєчасного реагування регулятора електронних ресурсів на шахрайство та дезінформацію щодо правомірності здійснення фінансових потоків між користувачами.

Об'єктивно складна ситуація в банківській системі загострюється тією обставиною, що перехід економіки на цифрові рейки метапростору FinTech-послуг здійснюється надзвичайно швидкими темпами, практично не залишаючи часу на адаптацію до принципово нової реальності. Ці обставини змушують банківський сектор інтегруватись у цифрову економіку, що включає в себе поступову відмову від готівкових транзакцій, розвиток нових видів платежів та переказів, впровадження мобільних додатків, безконтактних платежів, онлайн-кредитування, електронних грошей, використання штучного інтелекту тощо.

Аналіз останніх досліджень і публікацій. Проблемами забезпечення безпеки банківської системи шляхом управління фінансовими інструментами платіжних систем у потоці

розрахункових операцій займалися такі вчені як: Абрамова А. [1], Бахугуна А., Р.К. Бішт, Дж. Панд [2], М. Барр, А. Харріс, Л.А. Менанда, В. Сюй [4], А. Дадукіс, М.А. Фіашетт, Г. Фузі [6], Н.В. Доран, Р. Бедирча, О. Манто [7], які на методологічному рівні визначили аналітичний синтез між безпекою інформаційного простору банківських установ та регуляторами національної безпеки держави щодо захисту інтересів клієнтів. Формуванням концепції безпеки банківської системи та експериментальною перевіркою всіх її положень щодо хеджування ризиків електронних платіжних систем, які пов'язані зі інноваційними орієнтирами розвитку цифрових технологій займались такі вчені, як П. Хуо, Л. Ван [12], А. Джавед, М. Лакоджу, П. Бернап, О. Рана [16], Е. Лайтсу, А. Каргас, Д. Варутас [17], Н. Трусова, І. Чкан [23; 24], Н. Кондрацька [26].

Формулювання цілей статті. Метою нашого дослідження є розробка методичного підходу та практичних рекомендацій щодо забезпечення безпеки банківської системи за регуляторними стабілізаторами СЕП НБУ, які на засадах метапростору FinTech-послуг нівелюють загрози платіжних систем в банківському інформаційному просторі, стабілізують захист учасників та користувачів платіжного портфеля банківських установ від дезінформації та шахрайства.

Виклад основного матеріалу дослідження. Забезпечення безпечного, стійкого і стабільного розвитку банківської системи України набуває особливої значимості, враховуючи, що її функціонування в сучасних умовах ускладняється появою кризових явищ у різних сферах економіки. Банківська діяльність завжди пов'язана з ризиком, можливим витоком інформації, наявністю внутрішніх та зовнішніх загроз. Банки є основними суб'єктами фінансового ринку, тому їх безпека сьогодні на першому плані, оскільки вирішення концептуальних питань їх діяльності зумовлено активним провадженням цифровізації інноваційних технологій метапростору та дією наявних в Україні структур економічної розвідки з питань міжнародної організованої злочинності. Цифровізація дозволяє користуватися усіма перевагами процесу втілення довгострокових та короткострокових планів реалізації цифрової трансформації банківської системи на засадах метапростору Fintech-послуг задля руху електронних грошей із високою мобільністю, автоматизації фінансових операції із математичним алгоритмам їх дії, нівелювання затрат на виготовлення та зручність безпечного користування серверами, що стикаються із постійною спробою шахраїв та хакерів заволодіти ними [25].

Методологічна платформа безпекового концепту розвитку банківської системи в мережі електронних платіжних систем в єдиному кібернетичному захисному метапросторі FinTech-послуг дозволяє інтегрувати процеси автоматизованого використання платіжних серверів в світовому масштабі, і, таким чином, суттєво зменшити загрози банківських інформаційних ресурсів через синергізм та ознаки гібридності.

Пріоритетним напрямом підвищення безпеки банківської системи та її електроно-платіжного ландшафту в цілому – створення сучасних методів і засобів захисту від гібридного нападу на банківські об'єкти обслуговування учасників та користувачів платіжних систем в інфраструктурі НБУ.

З єдиних позицій безпеки банківської системи, запропоновано методичний підхід, який дозволяє визначити рівень ієрархії банківського обслуговування учасників та користувачів Системи електронних платежів Національного банку України (СЕП НБУ) на основі комплексного оцінювання об'єктів загроз в метапросторі FinTech-послуг, а саме: інформаційної безпеки (IS), безпеки оверсайту платіжних систем (SOPS), безпеки платіжного портфеля банківських установ (SPPB). Він включає в себе: побудову інтегрованої цілісної моделі, яка будується на платформі FinTech-послуг при зміні банківських інформаційних ресурсів за умови визначення ймовірності впливу загроз на об'єкти IS, SOPS, SPPB, що забезпечують обслуговування учасників та користувачів СЕП НБУ; індикатори захисту банківських інформаційних ресурсів на умовах оверсайту платіжних систем та платіжного портфеля банківських установ на фінансовому ринку для забезпечення безпеки СЕП НБУ.

На етапі інтегрованої цілісної моделі при зміні банківських інформаційних ресурсів за умови визначення ймовірності впливу загроз на об'єкти IS, SOPS, SPPB, що забезпечують

обслуговування учасників та користувачів СЕП НБУ, необхідним є оцінювання інтенсивності нормування метричних коефіцієнтів загроз на основі існуючого класифікатора [20]. Серед складових класифікатора загроз в метапросторі FinTech-послуг щодо обслуговування учасників та користувачів СЕП НБУ виділено наступні:

– безпека банківських інформаційних ресурсів (БІР): IS, SOPS, SPPB;

– характер напрямків безпека банківських інформаційних ресурсів: нормативно-правовий, організаційний, інженерно-технічний;

– особливості інформації: конфіденційність, цілісність, доступність;

– ієрархія рівнів банківського обслуговування учасників та користувачів СЕП НБУ: *FL* – фізичний рівень, *NL* – мережевий рівень, *OSL* – рівень операційних систем, *DBL* – рівень систем управління базами даних, *BL* – рівень банківського технологічного обслуговування та сервісів. Для оцінювання загальної величини загроз на об'єкти обслуговування IS, SOPS, SPPB в СЕП НБУ необхідно використовувати ресурс FinTech-послуг [13-14; 21].

Для попередження або знешкодження *i*-ї загрози в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ запроваджується відповідні FinTech-послуг, які ідентифікуються за формулами (1)-(3):

FinTech-послуга конфіденційності:

$$w_i^c \alpha_i^c = \frac{1}{K} \alpha_i^c \sum_{k=1}^{K} w_{ik}^c, \quad (1)$$

де, w_{ik}^c – експертний ваговий коефіцієнт конфіденційності FinTech-послуги через банківську установу щодо попередження або знешкодження *i*-ї загрози в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ; α_i^c – ваговий коефіцієнт прояву атаки і-ї загрози та її виникнення за FinTech-послугою конфіденційності функціонування ієрархії банківського обслуговування учасників та користувачів СЕП НБУ.

послуга цілісності:

$$w_i^l \alpha_i^l = \frac{1}{K} \alpha_i^l \sum_{k=1}^{K} w_{ik}^l, \quad (2)$$

де, w_{ik}^l – експертний ваговий коефіцієнт цілісності FinTech-послуги щодо попередження або знешкодження і-ї загрози в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ; α_i^l – ваговий коефіцієнт прояву атаки *i*-ї загрози за FinTech-послугою цілісності в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ.

послуга доступності:

$$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A, \quad (3)$$

де, w_{ik}^A – експертний ваговий коефіцієнт доступності FinTech-послуги щодо попередження або знешкодження і-ї загрози в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ; α_i^A – ваговий коефіцієнт прояву атаки *i*-ї загрози в метапросторі FinTech-послуг доступності в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ.

Оцінювання декількох загроз на певну послугу в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ визначається за формулами (4)-(6):

послуга конфіденційності:

$$w_{synerg}^c = \sum_{i=1}^{M} w_i^c \alpha_i^c, \quad (4)$$

послуга цілісності:

$$w_{synerg}^l = \sum_{i=1}^{M} w_i^l \alpha_i^l, \quad (5)$$

послуга доступності:

$$w_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A, \quad (6)$$

де, M – кількість загроз, які вибрані експертом FinTech-послуг із їх сукупності в класифікаторі (ISO/IEC 27001), щодо об'єктів IS, SOPS, SPPB, які уособлюють банківські інформаційні ресурси для обслуговування учасників та користувачів СЕП НБУ (тобто $M \le N$).

Визначення сумарної величини загроз за об'єктами IS, SOPS, SPPB в банківських інформаційних ресурсах, які обслуговують учасників та користувачів СЕП НБУ:

$$w_{synerg}^{IS} = \sum_{i=1}^{N} (w_i^c \cap w_i^l \cap w_i^A \cap w_i^{Au}) \times \alpha_i, \quad (7)$$

$$w_{synerg}^{SOPS} = \sum_{i=1}^{N} (w_i^c \cap w_i^l \cap w_i^A \cap w_i^{Au}) \times \alpha_i, \quad (8)$$

$$w_{synerg}^{SPPB} = \sum_{i=1}^{N} (w_i^c \cap w_i^l \cap w_i^A \cap w_i^{Au}) \times \alpha_i, \quad (9)$$

Оцінювання узагальненої синергетичної загрози в метапросторі FinTech-послуг за об'єктами банківських інформаційних ресурсах (IS, SOPS, SPPB), які обслуговують учасників та користувачів СЕП НБУ проводиться за формулою (13):

$$w_{synerg}^{IS,SOPS,SPPB} = w_{synerg}^{IS} \cup w_{synerg}^{SOPS} \cup w_{synerg}^{SPPB}, \quad (10)$$

Синергетичність загроз в метапросторі FinTech-послуг через банківські установи, які обслуговують учасників та користувачів СЕП НБУ з урахуванням їх гібридності визначається за формулою (11):

$$w_{synerg}^{hubrid\ c,l,A,Au} = w_{synerg}^{c} \cap w_{synerg}^{l} \cap w_{synerg}^{A}, \quad (11)$$

На наступному етапі, за результатами комплексного оцінювання загроз в метапросторі FinTech-послуг за об'єктами банківських інформаційних ресурсів (IS, SOPS, SPPB) в модельній ієрархії банківського обслуговування учасників та користувачів СЕП НБУ – $G^{SEPNBU} = \{O^{SEPNBU}\}\{L^{SEPNBU}\}\{I_A\}$ визначаються індикатори захисту фінансових ресурсів за умови оверсайту платіжних систем та платіжного портфеля банківських установ на фінансовому ринку для забезпечення кібербезпеки СЕП НБУ.

Це передбачає за такими напрямами:

визначення зв'язку між безпекою оверсайту платіжних систем в активах банківських інформаційних ресурсів $\{I_A\}$ та елементами ієрархії FinTech-послуг щодо банківського обслуговування учасників та користувачів СЕП НБУ G^{SEPNBU}. Кожен елемент описується вектором, який представлено у формулі (12).

$$I_A = (SOPS_{type}, A^C, A^I, A^A, C_Y), \quad (12)$$

де, $SOPS_{type}$ – тип активу банківських інформаційних ресурсів, який описується множиною базових параметрів безпеки оверсайту платіжних систем (формула (13)):

$$Type = \{BT, PID, RrD, KT, StO, Ol, YI, PD\}, \quad (13)$$

де, BT – банківська таємниця; PID – платіжні документи; KrD – кредитні документи; KT – комерційна таємниця; StO – статистичні дані; Ol – загальнодоступна інформація; YI – керуюча інформація; PD – персональні дані; A^C – конфіденційність; A^I – цілісність; A^A – доступність; C_Y – безперервність інформації (інформація, яка забезпечена захистом від злочинного шахрайства). Вони набувають значення 1 – якщо інформація необхідна, 0 – в іншому випадку.

визначення зв'язку між активами банківських інформаційних ресурсів та об'єктами середовища безпеки платіжного портфеля банківських установ в метапросторі FinTech-послуг щодо для забезпечення кібербезпеки СЕП НБУ. Кожен елемент $O_l \in \left\{O^{SEP\,NBU}\right\}$, описується вектором (формула (14)):

$$O_l = \left\{Y^{SPPB}, IO\right\}, \tag{14}$$

де, $Y^{БСІПР}$ – рівень забезпечення безпеки банківського обслуговування в метапросторі FinTech-послуг за інформаційними ресурсами платіжного портфеля банківських установ в загальній системі безпеки СЕП НБУ, яка визначається наступною множинною величиною (формула (15)):

$$Y^{SPPB} = \{FL, NL, OSL, DBL, BL\}, \tag{15}$$

де, FL – фізичний рівень; NL – мережевий рівень; OSL – рівень операційних систем; DBL – рівень систем управління базами даних; BL – рівень банківського технологічного обслуговування та сервісів.

Для визначення типу зв'язку та існуючого відношення $IO^{Y^{БСІПР}}$ між активами банківських інформаційних ресурсів та об'єктами середовища безпеки платіжного портфеля банківських установ загальній системі безпеки СЕП НБУ використовується правило (формула (16)):

$$IO^{Y^{SPPS}} \left\| IO_{il}^{\mathrm{Y}^{\mathrm{SPPS}}} \right\|, \tag{16}$$

де, $IO_{il}^{\mathrm{Y}^{\mathrm{SPPB}}}$ – тип наявного зв'язку між *i*-м банківських інформаційних ресурсом та l-м об'єктом середовища безпеки платіжного портфеля банківських установ в загальній системі безпеки СЕП НБУ.

На основі запропонованої синергетичної моделі банківського обслуговування в метапросторі FinTech-послуг за інформаційними ресурсами платіжного портфеля банківських установ в загальній системі безпеки СЕП НБУ, із врахування сек'юритизації платіжного портфеля на фінансовому ринку для попередження загроз та забезпечення потреб учасників та користувачів, маємо вираз алгоритму (17):

$$GR^{SEP\ \ NBU} = \left\{ \left\{ DF^{SEP\ \ NBU}_{SPPB} \right\}, \{T_{risk}\}, \{T_p\}, \{T_U\}, \{VH\} \right\}, \tag{17}$$

де, $\left\{DF^{SEP\,NBU}_{SPPB}\right\}$ – множина джерел загроз в метапросторі FinTech-послуг за ієрархією банківського обслуговування учасників та користувачів СЕП НБУ, що сек'юритизує (захищає) платіжний портфель банківських установ на фінансовому ринку; $\{T_{risk}\}$ – якісний індикатор попередження загроз в метапросторі FinTech-послуг при сек'юритизації платіжного портфеля банківських установ на фінансовому ринку в ієрархії банківського обслуговування учасників та користувачів СЕП НБУ; $\{T_p\}$ – множина базових термів ймовірності виникнення загрози в *j*-му активі банківських інформаційних ресурсів розміщених в метапросторі FinTech-послуг; $\{T_U\}$ – множина базових термів отримання збитку від виникнення небезпечних обставин в банківському обслуговуванні учасників та користувачів СЕП НБУ; $\{VH\}$ – множина деструктивного стану об'єктів SPPB в модельній ієрархії банківського обслуговування учасників та користувачів СЕП НБУ, який використовує зловмисник представлена в алгоритмі (18):

$$GR^{SEP\ \ NBU}_{IA\ SPPB} = \left\{ aid_i, pur_i, T_{IA}, S_{\max\ i}, pr_j, MS^{SEP\ \ NBU}_{i} \right\} \forall\, i \in n, \forall\, j \in m, \tag{18}$$

де, aid_i – ідентифікатор зловмисника (категорія кібершахрайства), що зафіксована в метапросторі в метапросторі FinTech-послуг; pur_i – мета зловмисника; T_{IA} – час здійснення

загрози; $S_{\max_i}$ – ймовірнісний збиток від загроз в банківському обслуговуванні учасників та користувачів СЕП НБУ при кібератаці на платіжний портфель банківських установ; pr_j – ймовірність виникнення загрози в *j*-му активі FinTech-послуг на банківські інформаційні ресурси, які передбачені для сек'юритизації платіжного портфеля банківських установ на фінансовому ринку; $MS_i^{SEP\,NBU}$ – рекомендації щодо виявлення загроз в метапросторі FinTech-послуг та реагування технічних засобів захисту інформації (ТЗЗІ) на кібератаку та її впливу на платіжних портфель банківських установ.

Комплекс загроз має вигляд:

$$DF^{SEP\ \ NBU} = \left\{ V^{NS} \right\} \cup \left\{ V^{AS} \right\}, \tag{19}$$

$$V^{AS} = \left\{ V^{ASBI} \right\} \cap \left\{ V^{ASIB} \right\} \cap \left\{ V^{ASKB} \right\}, \tag{20}$$

Такий підхід дозволяє визначити зв'язок між джерелами загроз і об'єктами SPPB в метапросторі FinTech-послуг для захисту об'єктів банківського обслуговування СЕП НБУ $V^{DF} = \left\| a_{ij}^{DF} \right\|$.

Загальна ціна ризику на всі активи FinTech-послуг (банківські інформаційні ресурси), які задіяні в сек'юритизації платіжного портфеля банківських установ на фінансовому ринку для забезпечення безпеки СЕП НБУ розраховується за формулою (21)-(22):

$$R_{\substack{full\ \ risk \\ БСІПР}} = \sum_{j=1}^{n} R_j, \tag{21}$$

$$R_j = pr_j \times q_j, \tag{22}$$

де, pr_j – ймовірність виникнення ризику в *j*-му активі банківських інформаційних ресурсів при розподілі платіжного портфеля банківських установ на фінансовому ринку для забезпечення кібербезпеки СЕП НБУ; q_j – збиток.

Ймовірність виникнення ризику в активах FinTech-послуг (банківських інформаційних ресурсів) при розподілі платіжного портфеля банківських установ на фінансовому ринку для забезпечення кібербезпеки СЕП НБУ:

$$pr_j = 1 - \prod_{i=1}^{m} (1 - pr_{ij}), \tag{23}$$

Визначення індикатора захищеності СЕП НБУ при гібридному впливі загроз на об'єкти SPPB при розподілі платіжного портфеля банківських установ на фінансовому ринку для забезпечення кібербезпеки СЕП НБУ здійснюється на основі удосконаленої моделі рівня захищеності банківських інформаційних ресурсів в метапросторі FinTech-послуг:

$$GR_{БСІПР}^{SEP\ \ NBU} = \left\{ \begin{array}{l} \left\{ I_A^{БСІПР} \right\}, \left\{ O_{SPPB}^{SEP\ \ NBU} \right\}, \left\{ DF_{SPPB}^{SEP\ \ NBU} \right\}, \left\{ RR_{SPPB}^{SEP\ \ NBU} \right\}, \\ \left\{ SP_{SPPB}^{SEP\ \ NBU} \right\}, \left\{ ROP_{SPPB}^{SEP\ \ NBU} \right\}, \left\{ UP_{r_{SPPB}}^{SEP\ \ NBU} \right\} \end{array} \right\}, \tag{24}$$

де, $\left\{ I_A^{SPPB} \right\}$ – множина активів FinTech-послуг (банківських інформаційних ресурсів), передбачених для сек'юритизації платіжного портфеля банківських установ на фінансовому ринку та забезпечення безпеки СЕП НБУ; $\left\{ O_{SPPBP}^{SEP\,NBU} \right\}$ – множина елементів ієрархії банківського обслуговування учасників та користувачів СЕП НБУ; $\left\{ DF_{SPPB}^{SEP\,NBU} \right\}$ – множина джерел загроз в метапросторі FinTech-послуг на платіжний портфель банківських

установ при його розподілі в СЕП НБУ; $\left\{RR_{SPPB}^{SEP\,NBU}\right\}$ – множина регуляторів безпеки платіжного портфеля банківських установ та забезпечення безпеки СЕП НБУ; $\left\{SP_{SPPB}^{SEP\,NBU}\right\}$ – множина можливих технологій метапросторі FinTech-послуг щодо захисту інформації в процесі сек'юритизації платіжного портфеля банківських установ на фінансовому ринку та забезпечення безпеки СЕП НБУ; $\left\{ROP_{SPPB}^{SEP\,NBU}\right\}$ результат оцінки захищеності платіжного портфеля банківських установ на фінансовому ринку для забезпечення безпеки СЕП НБУ; $\left\{UP_{rSPPB}^{SEP\,NBU}\right\}$ – рівень захищеності платіжного портфеля банківських установ при його розподілі на фінансовому ринку та забезпечення безпеки СЕП НБУ.

У моделі використані такі типи зв'язку: MP – є механізм захисту, що забезпечує протидію її деструктивному впливу $VH_i \in \{VH\}$; NMP – немає механізму захисту для забезпечення протидії і-ї загрози.

Якщо для всіх $i = ma^{DFSP} = NMP$, тоді банківські інформаційні ресурси та їх цифрові технології в метапросторі FinTech-послуг не здатні захистити від деструктивного впливу кібератак платіжну систему, а тому для об'єктів сек'юритизації платіжного портфеля банківських установ на фінансовому ринку необхідно розробляти додаткові механізми та регулятори захисту СЕП НБУ.

Регулятори SPPB дозволяють також захистити платіжні системи банківських установ $\left\{RR_{SPPB}^{SEP\,NBU}\right\}$ для збільшення запасу пропускної спроможності СЕП НБУ – $\{R_{BBI}\}$. Вони диференційовані за рівнем виконання вимог SPPB згідно міжнародних стандартів безпеки $\{OV_{BBI}\}$ та за рівнем відповідності SPPB до вимог з множини національних стандартів безпеки $\{R_{BBI}\}$ – $\{IU_{BBI}\}$:

$$\left\{ RR_{SPPB}^{SEP\quad NBU} \right\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}, \tag{25}$$

Для оцінювання регуляторів $\left\{RR_{SPPB}^{SEP\,NBU}\right\}$ використовуються індикатори, які поділяються на два типу (ISA/IEC 62443; ISO/IEC 27001): перший тип – обов'язкові індикатори для виконання банківськими установами; другий тип – рекомендовані індикатори FinTech-послуг для виконання функцій захисту. Для оцінки обов'язкових індикаторів першого типу встановлюється наступна шкала ступеня їх виконання: «ні» – присвоюється значення, рівне нулю; «частково» – присвоюється значення 0,30; 0,45; або 0.75; «так» – присвоюється значення, рівне одиниці. Для оцінки рекомендованих індикаторів другого типу встановлюється наступна шкала ступеня їх виконання: «так» – присвоюється значення, рівне одиниці; «ні» – індикатор визначається як неоцінюваний та не враховується у формуванні результатів оцінки. В табл. 1 наведені критерії рівня безпеки СЕП НБУ при сек'юритизації платіжного портфеля банківських установ на фінансовому ринку за допомогою серверів FinTech-послуг.

Використання індикаторів за напрямами ($R_{BBI_1}, R_{BB_2}, R_{BBI_3}$), дозволяє розрахувати результативну величину – рівень безпеки СЕП НБУ за об'єктами банківських інформаційних ресурсів в метапросторі FinTech-послуг, що підвищують рівень SPPB (OV_{IU_I}). Оцінка результативного індикатора (OV_{IU_I}) формується з часткових індикаторів ($OV_{IU_{IJ}}$) та розраховується за формулою (26):

$$OV_{IU_i} = \frac{\sum_j R_{BBI_i}^{OV_{IU_{ij}}}}{j}, \tag{26}$$

Оцінка ступеня виконання вимог за напрямом (R_{BBI_1}) «поточний рівень SPPB» здійснюється за формулою (27):

$$R_{BBI1} = \min(OV_{БІТП}, OV_{БПТП}, OV_{ooIP}, OV_{opIP}), \quad (27)$$

де, OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку банківських інформаційних ресурсів та попереджують загрозу SPPB в метапросторі FinTech-послуг; $OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційним процесом SPPB в метапросторі FinTech-послуг; $OV_{БПТП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний процес SPPB в метапросторі FinTech-послуг; OV_{opIP} – оцінка рівня SPPB з використанням криптографічних засобів захисту інформації в метапросторі FinTech-послуг.

Таблиця 1

Рекомендовані критерії рівня безпеки СЕП НБУ

Оцінка індикатора	Критерій виставлення оцінки індикатора SPPB
за індикаторами першого типу за умовами документування та виконання вимог SPPB	
0	Вимоги індикатора SPPB не встановлені у внутрішньому сервері FinTech-послуг
0.30	Вимоги індикатора SPPB встановлені у внутрішньому сервері FinTech-послуг, але не виконуються
0.45	Вимоги індикатора SPPB встановлені у внутрішньому сервері FinTech-послуг, але не виконуються
0.75	Вимоги індикатора SPPB встановлені у внутрішньому сервері FinTech-послуг і виконуються майже в повному обсязі
1.0	Вимоги індикатора SPPB встановлені у внутрішніх документах аудиту і виконуються в повному обсязі
за індикаторами другого типу за умови документування та виконання вимог SPPB	
0	Вимоги індикатора SPPB не встановлені у внутрішньому сервері FinTech-послуг
1.0	Вимоги індикатора SPPB повністю встановлені у внутрішньому сервері FinTech-послуг
за індикаторами виконання лише вимог SPPB	
0	Вимоги індикатора SPPB не виконуються
0.65	Вимоги індикатора SPPB виконуються в неповному обсязі
1.0	Вимоги індикатора SPPB виконуються в повному обсязі

Джерело: побудовано за даними [3; 5; 9; 18–20]

Оцінка ступеня виконання вимог за напрямом (R_{BBI_2}) «керування SPPB» метапросторі FinTech-послуг визначається за формулою (28):

$$R_{BBI\ 2} = {}^{k}R_{BBI\ 2}\ \frac{\sum_{j=1}^{m} IU_{1j}}{j}, \quad (28)$$

де, $k_{R_{BBI_2}}$ – корегуючий коефіцієнт (табл. 2); j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог за напрямом (R_{BBI_3}) «рівень усвідомлення загрози SPPB» в метапросторі FinTech-послуг визначається за формулою (29):

$$R_{BBI\ 3} = {}^{k}R_{BBI\ 3}\ \frac{\sum_{j=1}^{m} IU_{2j}}{j}, \quad (29)$$

де, $k_{R\ BBI\ 3}$ – корегуючий коефіцієнт (табл. 2); j – номер приватного показника, $j=\overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують обробку банківських інформаційних ресурсів в метапросторі FinTech-послуг та попереджують загрозу SPPB визначається за формулою (30):

$$OV_{ooIP} = k_{ooIP} \frac{\sum_{j=1}^{m} IU_{3j}}{j}, \quad (30)$$

де, k_{ooIP} – корегуючий коефіцієнт (табл. 2); j – номер приватного показника, $j=\overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують банківський інформаційний процес SPPB в метапросторі FinTech-послуг, визначається за формулою (31):

$$R_{\substack{OV\ SPPB \\ BITP}} = k_{OV\ BITP} \frac{\sum_{j=1}^{m} IU_{4j}}{j}, \quad (31)$$

де, $k_{OV\ BITP}$ – корегуючий коефіцієнт (табл. 2); j – номер приватного показника, $j=\overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують банківський платіжний процес SPPB в метапросторі FinTech-послуг, визначається за формулою (32):

$$OV_{BITP} = k_{BITP} \frac{\sum_{j=1}^{m} IU_{5j}}{j}, \quad (32)$$

де, k_{BITP} – корегуючий коефіцієнт (табл. 2); j – номер приватного показника, $j=\overline{1,...,m}$.

Оцінка рівня безпеки SPPB з використанням криптографічних засобів захисту інформації визначається в метапросторі FinTech-послуг, визначається за формулою (33):

$$OV_{opIP} = k_{opIP} \frac{\sum_{j=1}^{m} IU_{6j}}{j}, \quad (33)$$

де, k_{opIP} – корегуючий коефіцієнт (табл. 2); j – номер приватного показника, $j=\overline{1,...,m}$.

Таблиця 2

Правила визначення коригувальних коефіцієнтів

Коригувальний коефіцієнт	**Кількість часткових індикаторів, оцінки яких дорівнюють нулю (повністю не виконуються)**		
$k_{R_{BBI_2}}$	0	1-12	більше 12
$k_{R_{BBI\ 3}}$	0	1-18	більше 18
k_{ooIP}	0	1-24	більше 24
$k_{OV\ BITP}$	0	1-30	більше 30
k_{BITP}	0	1-10	більше 10
k_{opIP}	0	1-17	більше 17
Коригуючий коефіцієнт	1	0.75	0.65

Джерело: побудовано за даними [3; 5; 9; 18–20]

Узагальнений індикатор – рівень безпеки СЕП НБУ дозволяє визначити відповідність технічних сервірів в метапросторі FinTech-послуг щодо захисту банківських інформаційних ресурсів на вимоги регуляторів SPPB та визначається за формулою (33):

$$OPP^{SEP\ NBU} = \sum_{i=1}^{k} OPP_i \ , \tag{33}$$

де, k – кількість часткових k індикаторів безпеки СЕП НБУ; OPP_i – частковий індикатор безпеки СЕП НБУ, що набуває значення з множини: OPP_1 – відсутність неприпустимих ризиків (якщо в СЕП НБУ при складанні моделі загроз в метапросторі FinTech-послуг (моделі дезінформації та шахрайства) виявлені неприпустимі за своїм рівнем ризики, тоді $OPP_1=0$, в іншому випадку – $OPP_1=1$); OPP_2 – відсутність небезпечних загроз безпеці СЕП НБУ (якщо запроваджується сервіри в метапросторі FinTech-послуг щодо захисту банківських інформаційних ресурсів SPPB, тоді $OPP_2=0$; якщо в СЕП НБУ при складанні моделі загрози в метапросторі FinTech-послуг виявлені «незапроваджені» механізми SPPB, тоді $OPP_2=1$); OPP_3 – рівень відповідності технічного сервіру FinTech-послуг щодо захисту банківських інформаційних ресурсів до вимог регуляторів SPPB (якщо рівень відповідає рекомендованим значенням, тоді $OPP_3=1$; якщо рівень відповідає нерекомендованим значенням, тоді $OPP_3=0$).

Таким чином, запропонований методичний підхід щодо забезпечення безпеки СЕП НБУ дозволяє підвищити рівень захисту банківських інформаційних ресурсів в метапросторі FinTech-послуг, отримати максимальну кількість емерджентних властивостей оверсайту платіжних систем при обслуговуванні учасників та користувачів в умовах гібридних загроз, пов'язаних із дезінформацією та шахрайством, а також попередження неефективних дій щодо сек'юритизації платіжного портфеля банківських установ на фінансовому ринку. Математичний інструментарій дозволяє оцінити синергію гібридності безпеки СЕП НБУ шляхом мінімізації витрат на банківський сервіс в платіжних системах за умови інтегрованого механізму цілісності, конфіденційності і достовірності банківських інформаційних ресурсів в метапросторі FinTech-послуг при використанні відкритих каналів зв'язку, а також оцінити їх функціональність в цілісній системі електронних платежів.

З позиції практичного використання платіжних систем, то в банківському сектоі використовуються електронні гроші (QIWI, WebMoney, VisaCash, PayPal, крипова люти), зокрема в ЄС анонсовано запуск цифрового євро [25]. Міністерство цифрової трансформації України ввело платформу «Дія. Підпис-EU» для цифрового підпису у застосунку «Дія», який визнається ЄС; створено нову програму для державних органів, відповідно до Закону України про е-резидентство; введено «Стратегію розвитку екосистеми інновацій в Україні» [27].

У 2021 р. НБУ відкрив проект «Е-гривня», метою якого є визначення потреби широкомасштабного випуску в Україні цифрової форми гривні [20]. Окрім виробленої концепції, цифрова трансформація банківської системи є можливістю для економічного зростання країни. Водночас, впровадження електронних грошей у приватних банківських установах має високий ступінь фінансового навантаження та ступінь ризику. Без належного курсу, гарантій та підтримки держави цифрова трансформація буде проводитися досить повільно, тому банківським установам, що функціонують в метапросторі Fintech-послуг, необхідністю впровадження потужний механізм інноваційних технологій, що дозволяють збільшувати швидкість здійснення обсягу фінансових операцій в умовах посиленої дії регуляторів НБУ та Європейського інвестиційного банку. Тобто, при зміні поведінки споживачів Fintech-послуг та зростаючого попиту на інноваційні технології метапростору в Fintech-послугах, змінюється кон'юнктуру банківського обслуговування СЕП НБУ у сукупності зі змінами правової бази. Це призводять до створення нових фінансових інструментів та регламентів у Fintech-послугах на банківське обслуговування учасників та користувачі СЕП НБУ.

Експерти вважають, що «пандемія та воєнний стан в країні тільки прискорили та активізували інноваційний метопростір FinTech-послуг» [29]. В 2020 р. НБУ ухвалив Стратегію розвитку Fintech-послуг в Україні до 2025 р., та з 2021 р. приєднався до Глобальної мережі фінансових інновацій (GFIN), що, зокрема, сприяло підвищенню рівня

проникнення інновацій метапростору до фінансового сектору та реалізації завдань розробленої Стратегії [11].

Розвитку метапростору Fintech-послуг в українській банківській системі значною мірою сприяє модернізація вітчизняної законодавчої бази та гармонізація її з європейським законодавством. Зокрема, прийняття Закону України «Про платіжні послуги» у 2021 р. було «проривом» для ринку платіжних послуг, наслідком чого було запровадження можливості випуску регулятором цифрової валюти (е-гривні), розширення набору платіжних послуг, поява нових категорій надавачів фінансових (платіжних) послуг, збільшення прозорості інформації для клієнтів, поява відкритого банкінгу та створення Open Banking API HUB в Україні. Важливим аспектом, що дозволяє активізувати та вивести з тіні вітчизняний ринок криптовалюти, вважається комплексним регулюванням ринку віртуальних активів, зокрема прийняття і ухвалення, не зважаючи на триваючу в країні війну, в 2022 р. Закону України «Про віртуальні активи», який набуде чинності після внесення змін до Податкового кодексу та адаптування його до стандартів ЄС в сфері регулювання криптовалютної індустрії [10]. Цей дозволяє визначити правовий режим послуг з обміну віртуальних активів, основних учасників ринку віртуальних активів, їх права та обов'язки, а також політику держави в сфері обігу віртуальних активів [9; 27; 28].

До повномасштабного воєнного конфлікту в Україні ринок FinTech-послуг налічував понад 200 компаній. Аналіз розподілу FinTech-послуг за сферами діяльності свідчить, що лідером у сфері фінансових технологій залишається технологічна інфраструктура, де безпосереднім продуктом є створення ІТ-рішень для банків і головною технологіє є API. Також суттєву частку (19%) займають платіжні сервіси та перекази. При цьому базовою технологією платіжних сервісів та продуктів з персональних фінансів став чат-бот [29]. Все більшої популярності набувають серед споживачів та користувачів банківських продуктів в інноваційному метапростоі FinTech-послуг – онлайн-кредитування, через швидкість та можливість оформлення позики в межах 24/7 та вимог до скорингу. Збільшилась активність інноваційних технологій метапростору із надання послуг щодо операцій криптовалюти із застосуванням Блокчейн, покращилась ситуація в сфері страхових послуг (InsurTech). При цьому найменш розвиненими нішами залишаються краудфандинг та сервіс порівняння FinTech-послуг [25]. Для створення продуктів з онлайн-кредитування, страхування та введення інноваційних фінансових інструментів українські банки застосовують технологію штучного інтелекту.

Технологія блокчейн як інновації метапростору значно змінила світ банків, надаючи підвищену безпеку, прозорість та управління ризиками у проведенні фінансових транзакцій. Постачальники FinTech-послуг швидко адаптували цю технологію, використовуючи її для створення смарт-контрактів, оптимізації торговельних та фінансових систем, що відкриває нові можливості для отримання прибутку. Впровадження ідентифікаторів на основі блокчейну, які впроваджені FinTech-установами допомогли підвищити безпеку фінансових транзакцій банків.

Загальний реєстр транзакцій і відстеження активів у бізнес-мережі Блокчейн матеріальних (будинок, автомобіль, готівка, земля) або нематеріальних (інтелектуальна власність, патенти, авторські права, брендинг), дозволяє зменшуючи ризики і скорочувати витрати для всіх учасників [5]. Технологія Блокчейн забезпечує безпеку реєстрів кредитної історії споживачів матеріальних і нематеріальних активів для банківського контролю в режимі реального часу і знижує ризики шахрайства. Завдяки використанню криптографії, децентралізації та механізмів консенсусу забезпечує довіра користувачів Системи Електронних Платежів (СЕП) НБУ до транзакцій. Крім того, СЕП на основі блокчейну дозволяють швидше, більш економно та індивідуально випускати цифрові цінні папери, усуваючи посередників та зменшуючи витрати, пов'язані з традиційними фінансовими операціями. Використовуючи узгоджені стандарти інноваційних технологій метапростору, протоколи та спільні процедури, Блокчейн забезпечує єдине джерело інформації для учасників банківської бізнес-мережі, керує даними та забезпечує простіший, дешевший і швидший доступ до капіталу через програмовані цифрові активи та цінні папери. Нові цінні папери можуть бути випущені

за лічені хвилини, а відповідні права та обов'язки закодовані та автоматизовані. Наприклад, Європейський інвестиційний банк (ЄІБ) випустив цифрову облігацію на публічній платформі блокчейн, використовуючи технологію метопростору щодо розподілення реєстру для розрахунків за цифровими облігаціями на суму 100 млн. EUR. Це усуває потребу використовувати Центральний Депозитарії Цінних Паперів та скоротити час розрахунків [8].

Світові витрати на блокчейн технології в банківському секторі збільшився в 2022 р. до 11.3 млрд. EUR, в 2024 р. прогнозується їх зростання до 18.2 млрд. EUR [9]. До 2025 р. більше половини світових банків будуть використовувати інноваційні технології метапростору в мережі Блокчейн для забезпечення безпеки та надійності фінансових транзакцій [9]. Згідно звіту Swiss Blockchain Federation, з 2020 р. більше 80% банків в Швейцарії використовують блокчейн технології для операцій з криптовалютою та іншими цифровими активами. Проте, згідно даних Chainalysis, з 2020 р. більше 60% усіх глобальних криптовалютних транзакцій були пов'язані зі злочинністю, з них 0.34% були пов'язані зі схемами відмивання грошей [15; 22]. Це свідчить про необхідність розробки FinTech-установами програм та математичних алгоритмів захисту використання блокчейн технологій в банквських продуктах та СЕП НБУ.

Висновки. Таким чином, забезпечення безпеки банківської системи та збалансованості перерозподілу грошової маси в економіці країни повинно здійснюватися на основі ефективного використання інструментів захисту банківських інформаційних ресурсів в системі електронних платежів, шляхом посилення механізму метапростору FinTech-послуг щодо грошових переказів, вартості FinTech-продуктів, які спрощують QR-платежі для учасників та користувачів платіжних систем, і зокрема, СЕП НБУ. Одним із інструментів, які можуть використовувати учасники СЕП НБУ як чинник формування помірного структурного дефіциту ліквідності банківських установ для контролювання кібенападів на платіжні системи є монетарний регулятор обов'язкових вимог. Він дозволяє удосконалити критерії СЕП НБУ шляхом диференціювання величини резервної грошової маси, внесеної на банківські депозити, за цільовою спрямованістю; зменшення обсягів обов'язкових резервів на величину довгострокових інвестиційних кредитів, які надані за рахунок самостійно сформованих ресурсів, величину придбаних ОВДП та депозитних сертифікатів НБУ; запровадження нарахування і сплати відсотків на величину обов'язкових резервів в платіжному портфелі банківських установ з метою підвищення ефективності здійснення платежів та переказів учасників СЕП НБУ.

Водночас, даний інструмент в грошово-кредитному регулюванні банківської системи не відноситься до числа операційних, а використовується лише в умовах виникнення структурних диспропорцій при банківському обслуговування користувачів та споживачів СЕП НБУ, і, така ситуація, за умови виникнення загрози кібернападу на банківські інформаційні ресурси може плинути на стабільність функціонування платіжних систем. Тому, на нашу думку, цей інструмент монетарного впливу доцільно трансформувати зі списку інструментів оперативного функціонування СЕП НБУ, до категорії інструментів довгострокового та структурного впливу на посилення механізму FinTech-послуг для захисту платіжних систем.

Цифрова трансформація банківської системи уможливлює рівень безпеки СЕП НБУ та економічне зростання країни. Інноваційний метапростір FinTech-послуг в мережі Блокчейн є сполучною ланкою між традиційними та новими фінансовими продуктами банків. Він спрощує інтеграцію банків зі світом кіберфізичних систем і цифрових активів, оптимізує фінансові операції є фундаментом для розвитку цифрових фінансів. Проте, легітимність блокчейну за умови консерватизму регуляторів призводить до розколу між державними та приватними блокчейн-платформами. Відповідно, модернізація законодавства щодо регулювання в банківській системі метапростору FinTech-послуг, в контексті подальшої цифровізації економіки, призведе до зміни регуляторів СЕП НБУ, які будуть мати цілісний зв'язок в банківською інформаційною платформою згідно вимог законодавства Європейської банківської системи у зв'язку з прагненням України стати членом ЄС та створити прозорі

умови для розбудови нової інфраструктури фінансового ринку, підвищення фінансової грамотності населення щодо фінансових інновацій та цифровізації послуг в майбутньому.

Список використаних джерел:

1. Abramova A. The risk system of commercial banks in conditions of digitalization. *Problems and prospects of management economics*. 2021. Vol. 4(28). P. 186–193.
2. Bahuguna A., Bisht R.K., Pande J. Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*. 2020. Vol. 29(5). P. 250–266.
3. Bakalynskyi O. Model and methods for determining the design characteristics of information security management systems. URL: https://www.researchgate.net/publication/348788054 (дата звернення: 07.11.2024).
4. Barr M.S., Harris A., Menand L., Xu W. Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy.* 2020. Vol. 1–28. URL: https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf (дата звернення: 07.11.2024).
5. Blockchain success. URL: https://www.ibm.com/topics/blockchain (дата звернення: 07.11.2024).
6. Dadoukis A., Fiaschetti M., Fusi G. IT adoption and bank performance during the Covid-19 pandemic. *Economics Letters*. 2021. Vol. 204.
7. Doran N.M., Bădîrcea R.M., Manta A.G. Digitization and financial performance of banking sectors facing Covid-19 challenges in central and eastern european countries. *Electronics (switzerland).* 2022. Vol. 11(21).
8. EIB issues its first ever digital bond on a public Blockchain. URL: https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain (дата звернення: 07.11.2024).
9. FAQs on a Digital Euro. URL: https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html (дата звернення: 07.11.2024).
10. Global Blockchain in finance sector. URL: https://www.computerworld.com/article/3356502/global-blockchain-spending-to-hit-124b-by-2022-finance-sector-leads-growth.html (дата звернення: 07.11.2024).
11. Global Network of Financial Innovations. 2021. National Bank of Ukraine. URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-priyednavsya-do-globalnoyi-mereji-finansovih-innovatsiy (дата звернення: 10.11.2024).
12. Huo P., Wang L. Digital economy and business investment efficiency: Inhibiting or facilitating? *Research in International Business and Finance*. 2022. Vol. 63. https://doi.org/10.1016/j.ribaf.2022.101797
13. ISA/IEC 62443. URL: https://www.isa.org/standards-and-publications/isa-standards/search (дата звернення: 10.11.2024).
14. ISO/IEC 27001. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 10.11.2024).
15. Is Bitcoin “Digital Gold”? The Value of Bitcoin. URL: https://www.moonpay.com/learn/bitcoin/bitcoin-digital-gold (дата звернення: 10.11.2024).
16. Javed A., Lakoju M., Burnap P., Rana O. Security analytics for real-time for ecasting of cyber attacks. *Software-practice and experience*. 2022. Vol. 52(3). P. 788-804.
17. Laitsou E., Kargas A., Varoutas D. Digital Competitiveness in the European Union Era: The Greek Case. *Economies.* 2020. Vol. 8(4).
18. Naderi E., Pazouki S., Asrari A. A remedial action scheme against false data injection cyber attack sin smart transmission systems: Application of thy ristor-controlled series capacitor (TCSC). *IEEE Transaction son Industrial Informatics*. 2022. Vol. 18(4). P. 2297-2309.
19. Roshan Y.E., Abdi Y. ICT and Information Asymmetry. New Evidence of the Financial System in Selected MENA Countries. *Iranian Economic Review*. 2022. Vol. 26(2). P. 445-458.
20. Stanikzai A.Q., Shah M. A. Evaluation of cyber security threats in banking systems. Paper presented at the 2021 IEEE Symposium Series on Computation al Intelligence, SSCI 2021 – Proceedings. DOI: https://doi.org/10.1109/SSCI50451.2021.9659862
21. The ICT Development Index (IDI): conceptual framework and methodology. *International Telecommunication Union.* URL: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016/methodology.aspx (дата звернення: 10.11.2024).
22. Towards the capital markets. URL: https://www.accenture.com/us-en/insights/capital-markets/capital-markets-vision-2025 (дата звернення: 10.11.2024).
23. Trusova N.V., Chkan I.A., Radchenko N.G., Yakusheva I.Y., Rubtsova N.N. Banking Innovations: Marketing Support in the Financial Market of Ukraine. *Economic Alternatives*. 2023. Vol. 2. P 384–408.
24. Trusova N.V., Chkan I.O., Kondratska N.M., Zakharova N.Yu., Osypenko S.O. Cybersecurity of the Banking Sector in the Context of Digitalization of the World’s Economy. *The Banking Law Journal*. 2023. Vol. 140(9). P. 471–502.
25. Кльоба Л.Г. Цифровізація – інноваційний напрямок розвитку банків. Електронне наукове фахове видання. *Ефективна економіка*. 2018. № 12. URL: http://www.economy.nayka.com.ua/pdf/12_2018/86.pdf (дата звернення: 07.11.2024).
26. Кондрацька Н.М. Фінансово-економічна безпека банківських установ: загрози та шляхи їх подолання. *Вісник Національного університету водного господарства та природокористування. Економічні науки*. 2019. № 4. С. 48–60.

27. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/ (дата звернення: 12.11.2024).

28. Національний банк України, «Е-гривня». URL: https://bank.gov.ua/ua/payments/e-hryvnia (дата звернення: 12.11.2024).

29. Українська асоціації ФінТех та інноваційних компаній (UAFIC). URL: https://fintechua.org/market-map (дата звернення: 12.11.2024).

References:

1. Abramova A. (2021). The risk system of commercial banks in conditions of digitalization. *Problems and prospects of management economics*, no. 4(28), pp. 186–193.

2. Bahuguna A., Bisht R. K., Pande J. (2020) Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*, no. 29(5), pp. 250–266.

3. Bakalynskyi O. (2020). Model and methods for determining the design characteristics of information security management systems. Available at: https://www.researchgate.net/publication/348788054 (accessed November 7, 2024).

4. Barr M. S., Harris A., Menand L., Xu W. (2020). Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy,* vol. 1-28. Available at: https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf (accessed November 7, 2024).

5. Blockchain Success. (2022). Available at: https://www.ibm.com/topics/blockchain (accessed November 7, 2024).

6. Dadoukis A., Fiaschetti M., Fusi G. (2021). IT adoption and bank performance during the Covid-19 pandemic. *Economics Letters*, no. 204.

7. Doran N. M., Bădîrcea R. M., Manta A. G. (2022). Digitization and financial performance of banking sectors facing Covid-19 challenges in central and eastern european countries. *Electronics (switzerland),* no. 11(21).

8. EIB issues its first ever digital bond on a public Blockchain. (2021). Available at: https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain.

9. FAQs on a digital euro. (2024). Available at: https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html (accessed November 7, 2024).

10. Global Blockchain in finance sector. (2022). Available at: https://www.computerworld.com/article/3356502/global-blockchain-spending-to-hit-124b-by-2022-finance-sector-leads-growth.html (accessed November 7, 2024).

11. Global Network of Financial Innovations. (2021). National Bank of Ukraine. Available at: https://bank.gov.ua/ua/news/all/natsionalniy-bank-priyednavsya-do-globalnoyi-mereji-finansovih-innovatsiy (accessed November 10, 2024).

12. Huo P., Wang L. (2022). Digital economy and business investment efficiency: Inhibiting or facilitating? *Research in International Business and Finance*, no. 63. DOI: https://doi.org/10.1016/j.ribaf.2022.101797

13. ISA/IEC 62443. Available at: https://www.isa.org/standards-and-publications/isa-standards/search (accessed November 10, 2024).

14. ISO/IEC 27001. Available at: https://www.iso.org/isoiec-27001-information-security.html (accessed November 10, 2024).

15. Is Bitcoin “Digital Gold”? The Value of Bitcoin. Available at: https://www.moonpay.com/learn/bitcoin/bitcoin-digital-gold (accessed November 10, 2024).

16. Javed A., Lakoju M., Burnap P., Rana O. (2022). Security analytics for real-time for ecasting of cyber attacks. *Software-Practice and Experience*, no. 52(3), pp. 788–804.

17. Laitsou E., Kargas A., Varoutas D. (2020). Digital Competitiveness in the European Union Era: The Greek Case. *Economies,* no. 8(4).

18. Naderi E., Pazouki S., Asrari A. (2022). A remedial action scheme against false data injection cyber attack sin smart transmission systems: Application of thy ristor-controlled series capacitor (TCSC). *IEEE Transaction son Industrial Informatics*, no. 18(4), pp. 2297–2309.

19. Roshan Y. E., Abdi Y. (2022). ICT and Information Asymmetry. New Evidence of the Financial System in Selected MENA Countries. *Iranian Economic Review*, no. 26(2), pp. 445–458.

20. Stanikzai A. Q., Shah M. A. (2021). Evaluation of cyber security threats in banking systems. Paper presented at the 2021 IEEE Symposium Series on Computation al Intelligence, SSCI 2021 – Proceedings. DOI: https://doi.org/10.1109/SSCI50451.2021.9659862

21. The ICT Development Index (IDI): conceptual framework and methodology. *International Telecommunication Union.* (2016). Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016/methodology.aspx (accessed November 10, 2024).

22. Towards the capital markets. (2020). Available at: https://www.accenture.com/us-en/insights/capital-markets/capital-markets-vision-2025 (accessed November 10, 2024).

23. Trusova N. V., Chkan I. A., Radchenko N. G., Yakusheva I. Y., Rubtsova N. N. (2023). Banking Innovations: Marketing Support in the Financial Market of Ukraine. *Economic Alternatives*, no. 2, pp. 384–408. (in Ukrainian)

24. Trusova N. V., Chkan I. O., Kondratska N. M., Zakharova N. Yu., Osypenko S. O. (2023). Cybersecurity of the Banking Sector in the Context of Digitalization of the World’s Economy. *The Banking Law Journal*, no. 140(9), pp. 471–502. (in Ukrainian)

25. Kloba L. G. (2018). Digitalization – an innovative direction of bank development. Electronic scientific professional publication. *Effective economy*, no. 12. Available at: http://www.economy.nayka.com.ua/pdf/12_2018/86.pdf (accessed November 7, 2024).

26. Kondratska N. M. (2019). Financial and economic security of banking institutions: threats and ways to overcome them. *Bulletin of the National University of Water Management and Environmental Management*. *Economic Sciences*, no. 4, pp. 48–60. (in Ukrainian)

27. Ministry of Digital Transformation of Ukraine. (2023). Available at: https://thedigital.gov.ua/ (accessed November 12, 2024).

28. National Bank of Ukraine, "E-hryvnia". (2022). Available at: https://bank.gov.ua/ua/payments/e-hryvnia (accessed November 12, 2024).

29. Ukrainian Association of FinTech and Innovation Companies (UAFIC). (2021). Available at: https://fintechua.org/market-map (accessed November 12, 2024).

Melnyk O. V., *Postgraduate Student*
Dmytro Motornyi Tavria State Agrotechnological University
alexreetwell@gmail.com
ORCID: 0009-0005-3990-6920

ENSURING THE SECURITY OF THE BANKING SYSTEM ON THE BASIS OF THE METASPACE OF FINTECH SERVICES

Abstract*. The article examines the processes of ensuring banking security on the basis of the FinTech services metaspace. A methodological approach to ensuring the security of the banking system is presented using the regulatory stabilizers of the NBU SEP, which, on the basis of the FinTech services metaspace, eliminate threats to payment systems in the banking information space, stabilize the protection of participants and users of the payment portfolio of banking institutions from disinformation and fraud. A synergistic model of security of the NBU SEP is proposed, taking into account the securitization of the payment portfolio of banking institutions in the financial market to prevent threats and meet the needs of participants and users in banking services. Criteria for the level of security of the NBU SEP are recommended. It is proven that the digital transformation of the banking system enables the level of security of the NBU SEP and the country's economic growth. The innovative FinTech services metaspace in the Blockchain network is a connecting link between traditional and new financial products of banks. It simplifies the integration of banks with the world of cyber-physical systems and digital assets, optimizes financial transactions and is the foundation for the development of digital finance. However, the legitimacy of Blockchain, provided that regulators are conservatism, leads to a split between public and private Blockchain platforms. Accordingly, the modernization of legislation on the regulation of the banking system of the metaspace of FinTech services, in the context of further digitalization of the economy, will lead to changes in the NBU's SEP regulators, which will have a holistic connection in the banking information platform in accordance with the requirements of the legislation of the European banking system in connection with Ukraine's desire to become a member of the EU and create transparent conditions for building a new financial market infrastructure, increasing the financial literacy of the population regarding financial innovations and digitalization of services in the future.*

Keywords: *security, banking system, metaspace, FinTech services, electronic payment system, payment portfolio, payment systems.*