
МІЖНАРОДНІ ФІНАНСИ

УДК 004.056:334.78

DOI: [https://doi.org/10.31617/zt.knute.2021\(119\)08](https://doi.org/10.31617/zt.knute.2021(119)08)

JEL Classification: G19, G21, G30, G38, O31

ЧУБАЄВСЬКИЙ Віталій

E-mail: chubaievskiy@knute.edu.ua

ORCID ID: 0000-0001-8078-2652

ВОЛОСОВИЧ Світлана

E-mail: s.volosovych@knute.edu.ua

ORCID ID: 0000-0003-3143-7582

к. політ. н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки Київського національного торговельно-економічного університету, директор Директорату стратегічного планування та європейської інтеграції Міністерства внутрішніх справ України
вул. Кіото, 19, м. Київ, 02156, Україна

д. е. н., професор, професор кафедри фінансів Київського національного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

БЕЗПЕКА КОРПОРАТИВНОЇ ІНФОРМАЦІЇ В ЕКОСИСТЕМІ *FINTECH*

Обґрунтовано, що застосування інструментів фінансових технологій обумовлює трансформацію інформаційних систем суб'єктів господарювання та забезпечення їхньої безпеки. Розглянуто екосистему FinTech у межах галузевого підходу як сферу використання інструментів фінансових технологій, послугами яких користуються суб'єкти господарювання, фізичні особи, органи державної влади. Проаналізовано подвійну природу кібербезпеки, що одночасно є складовою FinTech і забезпечує захист корпоративних інформаційних систем учасників екосистеми FinTech.

Ключові слова: корпоративні інформаційні системи, екосистема, фінансові технології, кібербезпека.

Постановка проблеми. Для забезпечення дієвої системи корпоративного управління необхідні інформаційні системи, що ефективно функціонують і задовольняють потреби користувачів усіх рівнів. За умов глобальної диджиталізації особливої актуальності набуває застосування інструментів фінансових технологій (*FinTech*) різними суб'єктами господарювання, зокрема оферентами фінансових послуг та їхніми споживачами. Це дає змогу споживачам отримувати фінансові послуги швидко, дистанційно та дешево за мінімальних вимог до переліку необхідних документів, що супроводжують надання

© Чубаєвський В., Волосович С., 2021

послуги. Завдяки модернізації фінансових послуг на основі інструментів *FinTech* оференти мають можливість розширювати коло своїх клієнтів. Водночас функціонування таких інформаційних систем може призвести до реалізації певних ризиків, що потребує створення ефективної системи протидії.

Аналіз останніх досліджень і публікацій. Проблематиці функціонування різних аспектів корпоративних інформаційних систем присвячено праці багатьох науковців. Зокрема Я. Лазор досліджував поняття та види корпоративних інформаційних систем [1]. Н. Орлова та Ю. Мохова розглянули завдання корпоративних інформаційних систем [2]. На вивченні питань функціонування екосистем *FinTech* зосереджувались учені А. Мазаракі [3], Г. Поченчук [4], Н. Радченко [5], А. Семенов, С. Цирулик [6] тощо. Х. М. Карім Алдухайдахаві, Ц. Чжан, М. Салам і М. Себай визначили вплив розвитку фінансових технологій на кібербезпеку [7]. Х. Наджаф, М. І. Мостафіз та Р. Наджаф проаналізували проблеми кібербезпеки в умовах посилення співпраці банків і *FinTech*-компаній [8]. Проте на сьогодні бракує досліджень, що стосуються вивчення можливостей застосування інструментів фінансових технологій суб'єктами господарювання, їх загроз та забезпечення безпеки для корпоративних інформаційних систем.

Метою статті є дослідження місця інструментів *FinTech* у корпоративній інформаційній системі, виявлення загроз їхнього використання та забезпечення безпеки їхнього функціонування.

Матеріали та методи. Теоретичним і методологічним підґрунтям дослідження є праці вітчизняних і закордонних науковців з питань функціонування корпоративних інформаційних систем та екосистем *FinTech*. Методи теоретичного узагальнення використано для визначення дефініції екосистеми *FinTech* з галузевого погляду; порівняльний аналіз і синтез – для обґрунтування застосування інструментів фінансових технологій суб'єктами господарювання, що обумовлює трансформацію інформаційних систем та гарантує їхню безпеку.

Результати дослідження. Основним функціональним призначенням інформаційних систем є забезпечення інформаційних процесів, як-от: створення, поширення, використання, збереження та знищення (утилізації) інформації [1]. Р. Бруханський зауважував, що інформаційне забезпечення є основою для задоволення потреби підприємства в необхідній інформації, обґрунтування управлінських рішень та стратегічного розвитку суб'єкта господарювання [9, с. 70]. Н. Орлова та Ю. Мохова виокремлюють головні завдання корпоративної інформаційної системи [2, с. 357], а саме:

- забезпечення максимально актуальною інформацією в найкоротші терміни;
- забезпечення багатоваріантності звітності, що орієнтовано на окремих суб'єктів різних рівнів корпоративного управління;
- використання в усіх звітах базового набору показників, що охоплюють найважливіші складові корпоративного управління.

Виконання цих завдань сприятиме розробці, прийняттю та реалізації ефективних стратегічних рішень суб'єктами господарювання.

На тлі пандемії відбулися кардинальні зміни поведінки споживачів на фінансових ринках, що підштовхнуло oferentів фінансових послуг до активізації цифрової трансформації [10, с. 6]. Підґрунтям цифрової трансформації є застосування інноваційних технологій на ринку фінансових послуг: великі дані, штучний інтелект, блокчейн, криптографія, біометрія, мобільний доступ, Інтернет. Це обумовлює трансформацію інформаційних систем суб'єктів господарювання та забезпечення їхньої безпеки. У бізнесі активізується використання послуг цифрового банкінгу, диджитал-страхування, платіжних платформ, залучення коштів через краудфандінгові платформи, інвестування. Водночас oferенти фінансових послуг можуть здійснювати господарську діяльність у різних сферах *FinTech*, зокрема *BankingTech*, *PayTech*, *WealthTech*, *InsurTech*, *CreditTech*, *PropTech*. Між інструментами, сферами *FinTech*, корпоративними інформаційними системами та їхньою безпекою існує міцний взаємозв'язок (рис. 1).

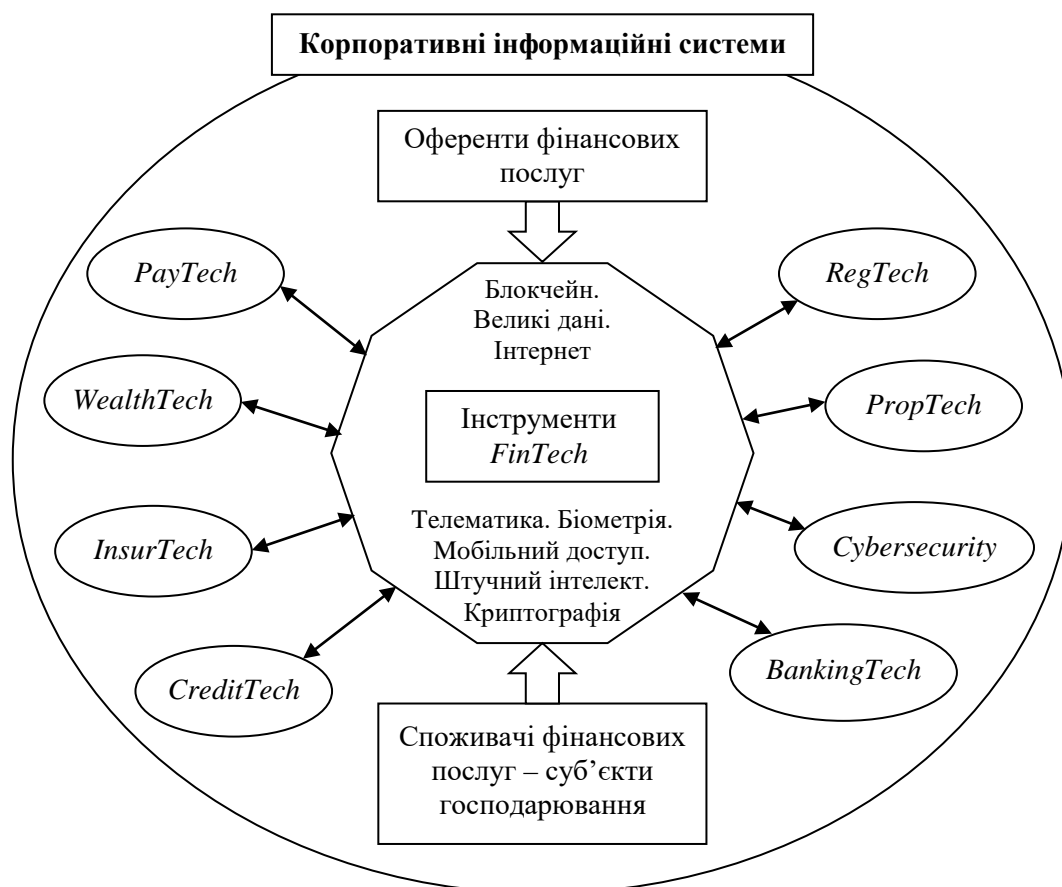


Рис. 1. Співвідношення між інструментами, сферами *FinTech*, корпоративними інформаційними системами та їхньою безпекою

Джерело: складено авторами.

Розвиток фінансових технологій спрямований на побудову екосистем *FinTech*, що стимулює технологічні інновації, обумовлює зростання ефективності фінансових ринків, місцевих економік і поліпшення досвіду клієнтів через впровадження різноманітних цифрових сервісів. Г. Поченчук розглядає *FinTech* як складну екосистему [3, с. 51]. Під екосистемою *FinTech* у межах галузевого підходу розуміють сфери застосування інструментів фінансових технологій, послугами яких користуються суб'єкти господарювання, фізичні особи, органи державної влади. Екосистеми *FinTech* полегшують доступ суб'єктів господарювання до швидких і дешевих фінансових послуг з дотриманням правового забезпечення цих процесів. Зростання диджиталізації фінансових операцій стимулює залучення нових учасників до екосистем *FinTech* та зацікавленість інвесторів до вкладення коштів у розвиток інструментів фінансових технологій. Глобальні обсяги інвестицій у *FinTech* у 2019 р. порівняно з 2018 р. мали тенденцію до зростання, проте у 2020 р. через коронакризу вже спостерігається їхнє зменшення (табл. 1). Дані за I півріччя 2021 р. свідчать про поступове відновлення цього показника. Протягом 2019 р. – I півріччя 2021 р. частка глобальних інвестицій у *WealthTech* зростала.

Таблиця 1

**Структура глобальних інвестицій в *FinTech*
за період 2018 – I півріччя 2021 рр.**

Сфери	2018		2019		2020		I півріччя 2021	
	млрд дол. США	%	млрд дол. США	%	млрд дол. США	%	млрд дол. США	%
<i>PayTech</i>	49.9	33.74	113.3	52.60	27.8	22.88	19.0	19.39
<i>InsurTech</i>	29.1	19.68	14.1	6.55	16.5	13.58	7.1	7.24
<i>RegTech</i>	8.0	5.41	3.5	1.62	10.4	8.56	6.6	6.73
Кібербезпека	0.5	0.34	0.9	0.42	2.2	1.81	3.7	3.78
<i>WealthTech</i>	0.7	0.47	0.4	0.19	0.8	0.66	1.4	1.43
Блокчейн та криптовалюта	7.2	4.87	5.0	2.32	4.3	3.54	8.7	8.88
Інші	45.5	35.49	78.2	36.3	59.5	48.97	51.5	52.55
Разом	147.9	100.00	215.4	100.00	121.5	100	98.0	100.00

Джерело: складено авторами за [11].

Канали залучення до екосистеми *FinTech* суб'єктів господарювання пов'язані з напрямками їхньої фінансової діяльності: здійснення розрахунків з контрагентами, бюджетами та державними цільовими фондами; страхування підприємницьких ризиків; інвестування, кредитування (див. табл. 2).

Канали залучення суб'єктів господарювання до екосистеми *FinTech*

Напрями фінансової діяльності підприємства	Сфера	Оференти – учасники екосистеми <i>FinTech</i> , що надають фінансові послуги суб'єктам господарювання
Інвестиційна діяльність	<i>WealthTech</i>	Роботоконсультанти, <i>BigTech</i> -компанії
	Краудфандінг	Краудфандінгові платформи
	Криптовалютний ринок	Криптовалютні біржі, криптовалютні брокери
Кредитна діяльність	<i>CreditTech</i>	Краудлендінгові платформи; банки, що надають кредити з використанням інструментів <i>FinTech</i> ; <i>BigTech</i> -компанії
Розрахунки	<i>PayTech</i>	Інтернет-платформи, що надають платіжні послуги; банки, що надають платіжні послуги із застосуванням інструментів фінансових технологій
Страховання підприємницьких ризиків	<i>InsurTech</i>	<i>InsurTech</i> платформи, страхові компанії, що використовують інструменти <i>FinTech</i>

Джерело: складено авторами.

У процесі управління інвестиційними портфелями суб'єкти господарювання звертаються до послуг роботоконсультантів. Це стимулює зростання частки глобальних інвестицій у *WealthTech* (див. табл. 1). Інвестиційний роботоконсультант – це автоматизований інтернет-сервіс управління інвестиціями клієнта, підґрунтям функціонування якого є штучний інтелект і великі дані. Він дає можливість клієнту отримати автоматично сформований портфель диверсифікованих інвестицій. Бостонською фінансовою корпорацією *StateStreet* у партнерстві з каліфорнійським блокчейн-стартапом *PeerNova* створено блокчейн-рішення для відстеження транзакцій, які мають відношення до інвестиційних активів. Завдяки цьому корпорації матимуть можливість залучити додаткові активи для управління, поліпшити свій фінансовий стан і підвищити безпеку транзакцій.

Для фінансування інвестиційних проєктів підприємства переважно малого та середнього бізнесу користуються послугами краудфандінгових платформ. У 2019 р. глобальне альтернативне фінансування малого та середнього бізнесу в Інтернеті становило 35 млрд дол. США, а у 2020 р. – близько 53 млрд дол. США на тлі того, що частка коштів, залучених за допомогою краудфандінгу малим та середнім бізнесом у загальному обсязі краудфандінгу у 2020 р. становила 47 % проти 38 % у 2019 р. [12]. Підґрунтям функціонування краудфандінгових платформ є технологія блокчейн, що не лише спрощує процес укладення угод, але й підвищує їхню безпеку.

Поширюється застосування суб'єктами господарювання альтернативних платіжних рішень, що базуються на використанні інструментів

фінансових технологій. Результати опитування *Bottomline Technologies* «*B2B Payments and Working Capital Management Strategies*», проведеного серед компаній Північної Америки та Європи, засвідчують, що близько 50 % корпорацій застосовують або планують використовувати альтернативні платежі, зокрема 55 % – платежі у реальному часі, 44 % – автоматизовані клірингові центри та 35 % – вбудовані у платежі блокчейн-мережі [13]. При цьому малий бізнес робить акцент на ініціативах дебіторської заборгованості поряд з великим бізнесом, який фокусується на кредиторській заборгованості. Ці тренди посилились через пандемію *COVID-19*, яка сприяла збільшенню зацікавленості до платежів у режимі реального часу на тлі масових змін поведінки бізнесу та споживачів. Понад 70 % усіх глобальних операцій електронної комерції здійснюється за допомогою платежів на основі інструментів фінансових технологій [14]. Зростання альтернативних платежів створює нові можливості для глобального поширення електронної комерції, обсяг якої до 2025 р. прогнозно становитиме понад 24 трлн дол. США [15].

Особливої зацікавленості серед суб'єктів господарювання набуває відкритий банкінг. Водночас розширення екосистеми *FinTech* зумовлює забезпечення кібербезпеки інформаційних систем, оскільки підвищуються ризики несанкціонованого доступу. Результати досліджень засвідчують, що співпраця між банками та *FinTech*-компаніями послабила кібербезпеку [11]. За деякими дослідженнями, фінансовий сектор у 300 разів вразливіший до кібератак [16]. За таких обставин корпоративні інформаційні системи постійно стикаються із загрозами щодо зловмисного програмного забезпечення, фішингових атак, порушення даних, хмарної безпеки, безпеки програм.

Кібербезпека є особливою сферою фінансових технологій і забезпечується застосуванням окремих інструментів *FinTech*: машинним навчанням, технологією блокчейн, токенизацією, біометрією. Активізація використання інструментів *FinTech* сприяє зростанню обсягів глобальних інвестицій у кібербезпеку на тлі збільшення частки глобальних інвестицій у фінансові технології у період 2018 – I півріччя 2021 рр. за суттєвого скорочення кількості укладених фінансових угод (рис. 2).

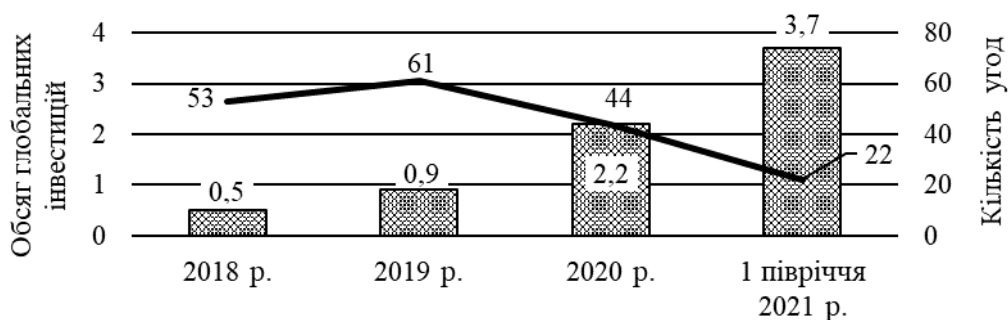


Рис. 2. Глобальні інвестиції в кібербезпеку за період 2018 – I півріччя 2021 рр.

Джерело: складено авторами за [11].

Посилення диджиталізації фінансової діяльності суб'єктів господарювання через пандемію *COVID-19* спричинило додаткові виклики для корпоративних інформаційних систем щодо реалізації кіберризиків. Протягом шести місяців після початку пандемії рівень шахрайства в інтернет-мережах збільшився на 60 % [17] на тлі того, що понад 4/5 оферентів фінансових послуг за відкриття рахунків виявляють шахрайські дії [18]. Це сприяло усвідомленню банками та платіжними операторами, що особисті дані клієнтів є їхньою корпоративною цінністю, тож для споживачів варто створити належні умови для володіння та контролю за ними [10, с. 11].

За звітом Світового банку та Кембриджського центру альтернативних фінансів (ССАФ) регулятори з усього світу визначили кібербезпеку як один з трьох ризиків, що загрожує учасникам екосистеми *FinTech* після коронавірусу, оскільки за час пандемії фінтех-провайдери зафіксували зростання загроз кібербезпеки на 15 % [19]. Водночас лише 29 % регуляторних органів зауважують, що було вжито адекватних заходів протидії цьому [19]. Програмою МВФ та *Bali Fintech Agenda* визнано необхідність вивчення центральними банками та наглядовими органами компонент управління ризиками *FinTech* [20].

Інструменти фінансових технологій, що використовують за надання фінансових послуг, не є досконалими. Великі дані, що забезпечують аналіз у реальному часі, та системи прийняття рішень несуть загрози несанкціонованого доступу та витоку даних. Технології розподіленої книги (*DLT*), що є основним засобом автентифікації користувачів та авторизації транзакцій, також мають певні ризики. Рішенням, що зроблені на основі такого мережевого рівня, властиві такі самі помилки програмного забезпечення та недоліки архітектури, що й іншому програмному забезпеченню. Водночас блокчейну без дозволу загрожують атаки 51 %.

Учені Х. М. Карім Алдухайдахаві, Ц. Чжан, М. Салам та М. Себай з'ясували, що зростання *FinTech* вплине на посилення кібербезпеки. Водночас ними визначено такі чинники впливу на стан кібербезпеки [8]:

- стан інформаційної безпеки;
- компетентність і вміння розробників та користувачів;
- рівень технологічної культури;
- самоефективність систем кібербезпеки.

За цих обставин зростає рівень кіберзахисту корпоративних інформаційних систем і оферентів фінансових послуг, що стане підґрунтям для забезпечення стабільної роботи фінансових ринків і підприємницьких структур.

Висновки. Важливим чинником зростання ефективності діяльності суб'єктів господарювання є споживання ними інноваційних фінансових послуг, що сприяють зростанню їхньої доступності, зменшенню їхньої вартості. Використання інструментів фінансових технологій, що є

підґрунтям надання таких послуг, зумовлює формування екосистем *FinTech*. Це впливає на виникнення додаткових ризиків функціонування корпоративних інформаційних систем. Забезпечення безпеки інформаційних систем є запорукою корпоративної стабільності. Завдання протидії кіберзагрозам стоїть не лише перед оферентами фінансових послуг, але й перед суб'єктами господарювання, що є їхніми споживачами, оскільки застосування інструментів фінансових технологій під час здійснення фінансових операцій призводить до ризиків для всіх учасників екосистеми *FinTech*. На нашу думку, кібербезпека має подвійну економічну природу. З одного боку, вона є складовою *FinTech*, з іншого – забезпечує захист корпоративних інформаційних систем учасників екосистеми *FinTech*. Одним з напрямів поліпшення безпеки корпоративних інформаційних систем є їхня сумісність з інформаційними системами оферентів фінансових послуг, що застосовують інструменти *FinTech*.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лазор Я. Поняття та види інформаційних систем. URL: <http://aphd.ua/publication-146>.
2. Орлова Н. С., Мохова Ю. Л. Впровадження інформаційних технологій в систему корпоративного управління. Відкрите освітнє е-середовище сучасного університету. 2017. № 3. С. 355-364. URL: https://elibrary.kubg.edu.ua/id/eprint/20078/1/N_Orlova_IKT_KU_FITU.pdf.
3. Мазаракі А. А., Волосович С. В. *FinTech*: монографія. Київ: Київ. нац. торг.-екон. ун-т, 2019. 308 с.
4. Поченчук Г. М. *FINTECH* у структурі фінансової системи. *Глобальні та національні проблеми економіки*. 2018. Вип. 21. С.49-55.
5. Радченко Н. Г. Перспективи розвитку *FinTech* для населення та бізнесу. *Економічні студії*. Вип. 1 (31). С. 122-126. 2021. № 1 (31). С. 122-126.
6. Семенов А. Ю., Цирулик С. В. Тенденції розвитку *Fintech*-послуг на світовому та вітчизняному ринках фінансових послуг. *Бізнес Інформ*. 2018. № 10. С. 327-324.
7. Hayder M. Kareem Al_Duhaidahawi, Jing Zhang, Mustafa S. Abdulreza, Meriem Sebai, Sinan Abdullah Harjan. Analysing the effects of *FinTech* variables on cybersecurity: Evidence form Iraqi Banks. *International journal of research in business and social science*. 2020. Vol 9. № 6. URL: https://www.researchgate.net/publication/346508094_The_Financial_Technology_Fintech_and_cybersecurity.
8. Khakan Najaf, Md Imtiaz Mostafiz and Rabia Najaf. Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*. 2021. Vol. 08, No. 02. URL: <https://www.worldscientific.com/doi/epdf/10.1142/S2424786321500195>.
9. Бруханський Р. Ф. Проблеми і пріоритети інформаційного забезпечення стратегічного менеджменту сільськогосподарських підприємств України. *Економічний аналіз: збірник наукових праць*. 2011. Вип. 9. Ч. 2, С. 69-71.
10. Мазаракі А., Волосович С. Домінанти ринку *FinTech* в умовах пандемії COVID-19. *Вісник Київського національного торговельно-економічного університету*. 2021. № 2. С. 4-19.
11. Pulse of *Fintech* H1'21. URL: [KPMG. home.kpmg/fintech](https://www.kpmg.com/au/issuesandinsights/articlespublications/2021/05/pulse-of-fintech-h1-21).

12. The 2nd Global Alternative Finance Market Benchmarking Report. URL: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/the-2nd-global-alternative-finance-market-benchmarking-report> URL: <https://www.crowdfunding-research.org/reports>.
13. *Fintech* gaining favour in B2B payments, Bottomline survey finds. URL: https://www.thepayers.com/e-invoicing-scf-e-procurement/fintech-gaining-favour-in-b2b-payments-bottomline-survey-finds/778910-24?utm_campaign=20190524-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content=.
14. Stefan Merz. Multiple ecommerce markets, one strategy: An exclusive interview with PPRO. URL: https://thepayers.com/interviews/multiple-ecommerce-markets-one-strategy-an-exclusive-interview-with-ppro--1243125?utm_campaign=20200624-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content=&utm_source=newsletter&utm_medium=Email&utm_term=&utm_content=&utm_campaign=.
15. The benefits of instant payment tech for insurance. URL: <https://www.itij.com/latest/long-read/benefits-instant-payment-tech-insurance>.
16. Cyberattacks are 300 times as likely to hit financial firms than other companies. A sweeping new report finds they're not prepared. Markets Insider. 2019. URL: <https://markets.businessinsider.com/news/stocks/cyberattacksimpact-major-threats-to-financial-firms-not-prepared-2019-6-1028296130>.
17. *COVID-19* to increase fraud rates by 60%, Feedzai's financial crime report finds. URL: https://thepayers.com/expert-opinion/major-acquisitions-in-the-payments-industry-2020-retrospective-part-i--1247102?utm_campaign=20210208-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content=&utm_source=newsletter&utm_medium=Email&utm_term=&utm_content=&utm_campaign=.
18. Four ways analysing digital behaviour can improve account opening fraud detection. URL: <https://thepayers.com/expert-opinion/four-ways-analysing-digital-behaviour-can-improve-account-opening-fraud-detection--1245113>.
19. The Global Covid-19 FinTech Regulatory Rapid Assessment Study. World Bank Group, e Cambridge Centre for Alternative Finance (CCAF) at the University of Cambridge Judge Business School. 2020. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf> <https://techmonitor.ai/techonology/cybersecurity/cybersecurity-risk-fintech-ecosystem>.
20. The Bali Fintech Agenda. IMF Policy Paper. Washington, D.C.: International Monetary Fund. 2018. URL: <https://www.elibrary.imf.org/view/journals/007/2018/050/article-A001-en.xml>.

Стаття надійшла до редакції 25.10.2021.

Chubaievskiy V., Volosovych S. Security of corporate information in FinTech ecosystem.

Background. *With the intensification of digitalization processes, the use of FinTech tools by various business entities, which include both financial service offerors and their consumers, is becoming especially important.*

Analysis of recent researches and publications. *The works of many scientists are devoted to the functioning of various aspects of corporate information systems. However, there is currently a lack of research on the feasibility of using financial technology instruments by business entities, their threats and security for corporate information systems.*

The aim of the article is to study the place of FinTech tools in the corporate information system, identify threats to their use and ensure the security of their operation.

Materials and methods. The theoretical and methodological basis of the study are the works of domestic and foreign scientists on the functioning of corporate information systems and FinTech ecosystems.

Results. The basis of digital transformation is the use of innovative technologies in the financial services market. This leads to the appropriate transformation of information systems of business entities and ensuring their security. There is an intensification of business use of digital banking services, digital insurance, payment platforms, raising funds through crowdfunding platforms, investing. The FinTech ecosystem within the sectoral approach should be understood as the areas of application of financial technology instruments, the services of which are used by various consumers, in particular, business entities, individuals, public authorities. The increasing digitalization of financial activities of business entities as a result of the Covid-19 pandemic has intensified the creation of additional challenges for corporate information systems for the implementation of cyber risks.

Conclusion. The use of financial technology tools by business entities leads to the formation of FinTech ecosystems. Ensuring the security of information systems is the key to corporate stability. The challenge of countering cyber threats is not only for financial service offerors, but also for business entities that are their consumers, as the use of financial technology tools in financial transactions causes risks to all participants in the FinTech ecosystem.

Keywords: corporate information systems, ecosystem, financial technologies, cybersecurity.

REFERENCES

1. Lazor, Ja. Ponjattja ta vydy informacijnyh system [Concepts and types of information systems]. Retrieved from <http://aphd.ua/publication-146> [in Ukrainian].
2. Orlova, N. S., & Mohova, Ju. L. (2017). Vprovadzhenja informacijnyh tehnologij v systemu korporatyvnogo upravlinnja [Introduction of information technologies into the corporate governance system] *Vidkryte osvitmje e-seredovyshhe suchasnogo universytetu – Open educational e-environment of a modern university*, 3, 355-364. Retrieved from https://elibrary.kubg.edu.ua/id/eprint/20078/1/N_Orlova_IKT_KU_FITU.pdf [in Ukrainian].
3. Mazaraki, A. A., & Volosovych, S. V. (2019). FinTech: Kyi'v: Kyi'v. nac. torg.-ekon. un-t [in Ukrainian].
4. Pochenchuk, G. M. (2018). FINTECH u strukturi finansovoi' systemy [FINTECH in the structure of the financial system]. *Global'ni ta nacional'ni problemy ekonomiky – Global and national economic problems*, (Issue 21), (pp.49-55) [in Ukrainian].
5. Radchenko, N. G. (2021). Perspektyvy rozvytku FinTech dlja naseleennja ta biznesu [Prospects for the development of FinTech for the population and business]. *Ekonomichni studii' – Economic studies*. (Issue. 1 (31), 1 (31), 122-126 [in Ukrainian].
6. Semenog, A. Ju., & Cyrulyk, S. V. (2018). Tendencii' rozvytku Fintech poslug na svitovomu ta vitchyznjanomu rynkah finansovyh poslug [Trends in the development of Fintech services in the global and domestic financial services markets]. *Biznes Inform – Business Inform*, 10, (pp. 327-324) [in Ukrainian].
7. Hayder, M. Kareem Al_Duhaidahawi, Jing, Zhang, Mustafa, S. Abdulreza, Meriem, Sebai, Sinan, & Abdullah Harjan (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International journal of research in business and social science*, (Vol 9), 6. Retrieved from https://www.researchgate.net/publication/346508094_The_Financial_Technology_Fintech_and_cybersecurity [in English].

8. Khakan, Najaf, Md Imtiaz, Mostafiz, & Rabia, Najaf. (2021). Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*, (Vol. 08), 02. Retrieved from <https://www.worldscientific.com/doi/epdf/10.1142/S2424786321500195> [in English].
9. Bruhans'kyj R. F. (2011). Problemy i priorityety informacijnogo zabezpechennja strategichnogo menedzhmentu sil's'kogospodars'kyh pidpryjemstv Ukrai'ny [Problems and priorities of information support of strategic management of agricultural enterprises of Ukraine]. *Ekonomichnyj analiz: zbirnyk naukovykh prac' – Economic analysis: a collection of scientific papers*, (Issue 9, part 2), (pp. 69-71) [in Ukrainian].
10. Mazaraki, A., & Volosovych, S. (2021). Dominanty rynku FinTech v umovah pandemii' COVID-19 [Dominants of the FinTech market in the context of the COVID-19 pandemic]. *Visnyk Kyi'vs'kogo nacional'nogo torgovel'no-ekonomichnogo universytetu – Herald of Kyiv National University of Trade and Economics*, 2, 4-19 [in Ukrainian].
11. Pulse of Fintech H1'21. Retrieved from KPMG. home.kpmg/fintech [in English].
12. The 2nd Global Alternative Finance Market Benchmarking Report. Retrieved from <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/the-2nd-global-alternative-finance-market-benchmarking-report> Retrieved from <https://www.crowdfunding-research.org/reports> [in English].
13. Fintech gaining favour in B2B payments, Bottomline survey finds. Retrieved from https://www.thepayers.com/e-invoicing-scf-e-procurement/fintech-gaining-favour-in-b2b-payments-bottomline-survey-finds/778910-24?utm_campaign=20190524-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content= [in English].
14. Stefan, Merz. Multiple ecommerce markets, one strategy: An exclusive interview with PPRO. Retrieved from https://thepayers.com/interviews/multiple-ecommerce-markets-one-strategy-an-exclusive-interview-with-ppro--1243125?utm_campaign=20200624-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content=&utm_source=newsletter&utm_medium=Email&utm_term=&utm_content=&utm_campaign= [in English].
15. The benefits of instant payment tech for insurance. URL: <https://www.itij.com/latest/long-read/benefits-instant-payment-tech-insurance>.
16. Cyberattacks are 300 times as likely to hit financial firms than other companies. A sweeping new report finds they're not prepared. Markets Insider. 2019. Retrieved from <https://markets.businessinsider.com/news/stocks/cyberattacksimpact-major-threats-to-financial-firms-not-prepared-2019-6-1028296130> [in English].
17. COVID-19 to increase fraud rates by 60%, Feedzai's financial crime report finds. Retrieved from https://thepayers.com/expert-opinion/major-acquisitions-in-the-payments-industry-2020-retrospective-part-i--1247102?utm_campaign=20210208-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content=&utm_source=newsletter&utm_medium=Email&utm_term=&utm_content=&utm_campaign= [in English].
18. Four ways analysing digital behaviour can improve account opening fraud detection. Retrieved from <https://thepayers.com/expert-opinion/four-ways-analysing-digital-behaviour-can-improve-account-opening-fraud-detection--1245113> [in English].
19. The Global Covid-19 FinTech Regulatory Rapid Assessment Study. World Bank Group, e Cambridge Centre for Alternative Finance (CCAF) at the University of Cambridge Judge Business School. (2020). Retrieved from <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf> Retrieved from <https://techmonitor.ai/techonology/cybersecurity/cybersecurity-risk-fintech-ecosystem> [in English].
20. The Bali Fintech Agenda. IMF Policy Paper. Washington, D.C.: International Monetary Fund. (2018). Retrieved from <https://www.elibrary.imf.org/view/journals/007/2018/050/article-A001-en.xml> [in English].