https://doi.org/10.31891/2307-5740-2022-304-2(2)-43
УДК 339.9+338.2:330.34

Алла ШЛАПАК
Київський національний економічний університет імені Вадима Гетьмана
https://orcid.org/0000-0001-8697-7039
e-mail: allashlapak@gmail.com

НАГЛЯДОВИЙ ПОТЕНЦІАЛ ФІНАНСОВИХ УСТАНОВ У ПРОТИДІЇ КІБЕРЗЛОЧИНАМ ТА ІНФОРМАЦІЙНИМ АСИМЕТРІЯМ В УМОВАХ ЗРОСТАННЯ РОЛІ FINTECH І BIG TECHS НА ЦИФРОВІЗОВАНИХ РИНКАХ КАПІТАЛУ

В статті доведено, що запит на цифровий суверенітет в межах національних юрисдикцій або на рівні інтеграційних об'єднань в умовах розширення кіберпростору і продукованих ним можливостей і загроз має кореспондуватись із потенціалом існуючої цифрової фінансової інфраструктури, яка є глобальною за своєю суттю, що наділяє FINTECH і BIG TECHS новими важелями впливу. Мета статті полягає у висвітленні наглядового потенціалу фінансових установ у протидії цифровій злочинності та інформаційним атакам в умовах зростання ролі FINTECH і BIG TECHS на міжнародних ринках капіталу. В статі ствердується, що посилення цифровізації глобальної економіки впливає на способи, в які банки виробляють і надають фінансові послуги своїм клієнтам, а також залучають Big Techs і FinTechs до цих процесів, що матиме революційні наслідки для існуючих фінансових установ і, особливо, традиційних банків. Виокремлено ряд потенційних причин, через які великі технологічні компанії можуть нарощувати свою присутність на ринках фінансових послуг. В статті досліджено ринок кібербезпеки і відзначено фактори, що спричиняють його розвиток і зростання. Продемонстровано, що багаторівневість встановлених взаємозв'язків між фінансовими установами та третіми сторонами ускладнює управління розповсюдженням внутрішньої інформації і загострює проблему інформаційної асиметрії, яка призводить до викривлення ринку і конкуренції. Аутсорсинг послуг, що здійснюється багатьма фінансовими установами, створює ризики концентрації для всього сектору. Фінансові установи все частіше використовують послуги хмарних провайдерів для зберігання даних. Дохід від хмарних послуг зазнає експоненціального зростання, але є лише декілька гравців, що мають достатній потенціал для обслуговування великих установ, що свідчить про олігополізацію даного ринку. Розглянуто «гейткіперську» роль фінансових установ, яка полягає у здатності відсіювати недостовірну інформацію, попереджувати фрод та інші зловживання, нести відповідальність за неупередженість і достовірність інформації. Висвітлено роль гейміфікації у розвитку ринку фінансових послуг під впливом FINTECH і BIG TECHS.

Досліджено зростання ролі BIG TECHS на ринку кредитування з огляду на зростання обсягів електронної комерції. Доведено, що зміни у фінансовому посередництві можуть суттєво вплинути на трансмісійні канали грошово-кредитної політики, що стане новим викликом для фінансових регуляторів і Центробанків, адже бізнес-модель Big Techs заснована на збиранні та використанні величезних масивів даних, але не для вирішення агентських проблем між кредиторами та позичальниками. Окреслене свідчить, що цифровізація ринків капіталу і банківської діяльності зокрема формує запит на посилення наглядової функції фінансових регуляторів задля мінімізації тактичних і системних ризиків, протидії кіберризиків, а також проявів інформаційної асиметрії на ринку фінансових послуг, що надаються BIG TECHS і FINTECHS.

Ключові слова: ринок кібербезпеки BIG TECHS, FINTECHS, ринок фінансових послуг, фінансовий нагляд, інформаційні асиметрії, гейміфікація, цифровізовані ринки капіталу, цифровий суверенітет ЄС, кредитування

Alla SHLAPAK
Kyiv National Economic University named after Vadym Hetman

SUPERVISORY CAPACITY OF FINANCIAL INSTITUTIONS IN COUNTERING CYBERCRIME AND INFORMATION ASYMMETRIES IN THE CONDITIONS OF THE GROWTH OF THE ROLE OF FINTECH AND BIG TECHS IN THE DIGITALIZED INTERNATIONAL CAPITAL MARKETS

The request for digital sovereignty within national jurisdictions or at the level of integration associations in the context of the expansion of cyberspace and the opportunities and threats it produces should correspond with the potential of the existing digital financial infrastructure, which is global in nature, which gives FINTECH and BIG TECH tools for transformative construction of the financial market. services. The purpose of the article is to reveal the supervisory potential of financial institutions in countering digital crime and information asymmetries in the context of the growing role of FINTECH and BIG TECHS in international capital markets. The article explores the role of FINTECH and BIGTECH as a dynamically developing segment at the intersection of the financial services and technology sectors. In it, technology startups and new market entrants are taking innovative approaches to products and services currently provided by the traditional financial services sector.

Today, new technologies (digital, telecommunications, biometrics, etc.) are reshaping the financial services industry, actively replacing traditional players and traditional business models. The integration of new financial solutions allows you to change the structure of consumption, reduce the cost of certain functionality (processing customer bases, loyalty programs, etc.), increase the efficiency and quality of business processes (targeting the target audience, scoring, etc.), and also significantly affect sustainability development of core business, etc. As a result, the financial technology industry is gradually turning into an independent, intensively developing sector of the modern economy. The FINTECH segment is rapidly developing, disrupting the usual order of things in the traditional value chain. Companies in the segment, using the latest technologies and new directions of activity, are reshaping the competitive landscape, blurring the boundaries that have been established among players in the financial services sector. The FINTECH ecosystem includes such elements as startups, technology companies, financial institutions and

infrastructure players. FINTECH platforms operate in the most profitable part of the banking chain. Most companies in the financial technology sector operate at the so-called last mile stage, that is, at the stage of interaction with the end consumer. These services include: P2P lending platforms, money transfer and payment acceptance services for small and medium enterprises. It is these areas that are the main sources of income for traditional banks. The very financing of the FINTECH industry is often of a credit nature, and cheap borrowed resources only increased interest in such innovations. of great importance for the fintech industry is the dynamically developing e-commerce market. In particular, this factor will stimulate the growth of the volume of services in the segment of payments and transfers, as well as in the segment of financing.

The article considers the phenomenon of gamification (the use of game elements), which is essentially a system of motivation and incentives, which leads to the fact that the client interacts with the financial institution more often, which makes it possible to achieve increased loyalty to the company. In the era of total digitalization, the problem of cybersecurity, protection of personal data, identification and authentication of a person in the information space when making financial transactions becomes relevant. The attention is focused on the risks of cyberattacks and theft of funds due to the disclosure of access to information systems.

Key words: cybersecurity market, BIG TECHS, FINTECHS, financial services market, financial supervision, information asymmetries, gamification, digital capital markets, EU digital sovereignty, lending and loans

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Постачальники фінансових послуг, які у більшості випадків не розробляють технологій, що лежать в основі останніх, дедалі частіше делегують реалізацію частини функцій виконавцям поза межами фінансового сектору, що призводить до зростання ролі тих гравців фінансового ринку, які не підпадають під нагляд фінансових регуляторів, що саме по собі ускладнює контроль за формуванням ланцюжка створення вартості. Такі IT-послуги, як хмарне зберігання та розробка додатків, є такими, що найчастіше передаються підрядникам [1]. Водночас, фінансовий провайдер, що використовує нову технологію, може бути недостатньо обізнаним в новій технології, що впроваджується (наприклад, розроблені алгоритми) з тим, аби ідентифікувати вразливість цифрових послуг, незалежно від того, чи є збої в роботі додатків навмисними чи ненавмисними. Це означає, що фінансовим установам важче контролювати весь ланцюжок створення вартості, що лежить в основі надання послуги. Це призводить до зростання операційних ризиків, адже більш складний ланцюг створення вартості у фінансовому секторі також ускладнює для наглядових органів реалізацію функцій контролю, виявлення ризиків та вчасне втручання на тих етапах, коли це необхідно. При цьому нові технології уможливлюють більший доступ до фінансових послуг навіть без необхідного для цього мінімального рівня компетентності в останніх та знання правових основ їхнього застосування. Однак цифровізований фінансовий ринок нарощує присутність учасників, що мають зловмисні наміри, і використовують переваги легкості доступу, щоб ввести інвесторів в оману і обійти правила контролю при відмиванні грошей або. Великі технологічні компанії, відомі як big techs, відіграють важливу роль у розподілі фінансових продуктів, хоча де-юре не мають зобов'язання діяти в інтересах споживача. Завдяки рекламним кампаніям big techs збільшують свою присутність в ланці розподілу фінансових продуктів, що робить їх фактичними монополістами на цифрову рекламу. Що стосується бек-офісу, великі технологічні компанії домінують на ринку хмарних сховищ, і саме вони забезпечують методи аналізу великої кількості даних. Очікується, що вони будуть використовувати свої компетенції у сфері маркетингу для подальшої спеціалізації своїх рекламних послуг, що дозволить їм зміцнити свої позиції у ланцюгу створення вартості. Чи будуть big techs переходити до надання всього комплексу суміжних фінансових послуг, поки залишається відкритим питанням. Втім якщо на європейському ринку не очікується, що вони повністю приймуть на себе функції банків та страховиків, на китайському ринку такий перехід вже відбувся. Big techs пов'язують між собою клієнтів та існуючих постачальників фінансових послуг, не здійснюючи самі діяльність, яка вимагає отримання відповідних ліцензій. Наприклад, у деяких країнах можна здійснювати платежі або перевіряти банківські залишки за допомогою програми Facebook Messenger. Amazon пов'язує платіжні, кредитні та страхові послуги зі своїми продуктами. У Нідерландах, наприклад, клієнти ING та Rabobank можуть користуватися деякими банківськими послугами за допомогою Google Assistant [2]. Ліцензовані фінансові установи продовжуватимуть нести остаточну відповідальність за послуги, що надаються споживачам, також у разі, коли значна частина їхніх ділових операцій передається підрядникам або пропонується клієнтам через інших гравців. Збільшення кількості гравців у ланцюжку створення вартості актуалізують проблему важливості фінансового нагляду в умовах тінізації глобальної економіки. Окрім фінансових та безпекових аспектів, актуальність кібербезпеки посилюється з позицій стратегічних геополітичних міркувань, для яких характерним є зростання напруженості через дискусії навколо межі прийнятності глобальності та відкритості мережі Інтернет, а також контролю над технологіями (наприклад, аналітика даних, хмарні обчислення, 5G, блокчейн та шифрування) та використання даних (наприклад, імплементація «Загального положення про захист даних» у ЄС). Така напруженість відображається в рішучості урядів встановлювати «цифрові кордони» або впроваджувати заборону на використання певних програм і блокувати доступ до веб-сайтів. Кіберпростір все частіше використовується в політичних та ідеологічних цілях. Європейський Союз визнав кібербезпеку необхідною умовою побудови стійкої, зеленої та цифрової Європи. Лідерство ЄС у ланцюжках створення вартості технологій кібербезпеки має ключове значення для досягнення більшої стратегічної автономії. Європейська комісія просуває принцип «цифрового

суверенітету» як засіб досягнення лідерства та автономії ЄС у цифровій сфері. У цьому контексті цифровий суверенітет відноситься до здатності Європейського союзу діяти незалежно в цифровому світі і повинен інтерпретуватись як з позицій захисних механізмів (захист стратегічних компаній ЄС від поглинань за межами ЄС), так і з погляду наступальних інструментів (потужні державні програми сприяння цифровим інноваційним технологіям).

Аналіз останніх досліджень і публікацій

Як наголошується експертами PwC [3], Big Techs і FinTechs не лише впливають на фінансовий сектор, а й дедалі більше інтегруються з ним, що призводить до зростання їхньої взаємозалежності і формуванні нових каналів поширення ризиків. Наслідками такого зрощення технологічного і фінансового секторів, на переконання Т. Кулкарні [4], Г. Бучака Г. Матвоса, Т. Піскорського і А. Серу [5], стає не лише своєрідне розмивання спеціалізації, але й пришвидшення кризової трансмісії між установами, інвестиційні портфелі стають дедалі більш взаємопов'язаними. В дослідженнях експертів МВФ [6], KPMG [7], BCG [8] розкриваються не лише характеристики нової хвилі технологічних інновацій, яка прискорює зміни у фінансовому секторі, але й трансформаційний вплив fntech-індустрії на ринок фінансових послуг і механізми фінансового регулювання. В їхніх аналітичних оглядах наголошується, що компанії, які виходять у простір fntech – відомі фінансові установи, нефінансові корпорації та стартапи – повинні враховувати постійно мінливий характер регулювання та нагляду у своїх стратегіях, бізнес-плануванні та управлінні ризиками. С. Баур-Язбек, Дж. Фрікенштейн і Д. Медін [9] зауважують, що наглядові органи починають усвідомлювати необхідність розробки нормативно-правової бази, галузевих інструкцій і процесів нагляду, щоб гарантувати, що фінансовий сектор запроваджує необхідні процеси та системи для запобігання, виявлення та ефективного управління кібератаками. Регулятори, метою яких є забезпечення стабільності фінансового сектору, анонсують розробку відповідної нормативної бази для зміцнення кіберстійкості і відповіді на виклики, з якими стикаються фінансові установи та їхні клієнти.

Формулювання цілей статті

Запит на цифровий суверенітет в межах національних юрисдикцій або на рівні інтеграційних об'єднань в умовах розширення кіберпростору і продукованих ним можливостей і загроз має кореспондуватись із потенціалом існуючої цифрової фінансової інфраструктури, яка є глобальною за своєю суттю, що наділяє FINTECH і BIG TECHS новими важелями впливу. Мета статті полягає у висвітленні наглядового потенціалу фінансових установ у протидії цифровій злочинності та інформаційним асиметріям в умовах зростання ролі FINTECH і BIG TECHS на міжнародних ринках капіталу.

Виклад основного матеріалу

Ринок кібербезпеки є одним із найбільш швидко зростаючих ринків у світі, в першу чергу, завдяки переходу до цифрової економіки та усвідомленню пов'язаних з цим вразливостей. У дослідженні IBM X-Force зазначено, що в 2021 році 70% кібератак на фінансові компанії були спрямовані на банки, 16% – на страхові компанії, а 14% – на інші фінансові установи [10]. Згідно з опитуванням, проведеним Конференцією наглядових органів державних банків (CSBS) у вересні 2021 року, понад 80% банкірів оцінили ризик кібербезпеки як «надзвичайно важливий» і головний внутрішній ризик, який продукує як операційні, так і репутаційні ризики [11]. У 2021 році світовий розмір ринку кібербезпеки оцінювався приблизно в 148 млрд євро [12]. Проте існують альтернативні кількісні оцінки його масштабів, що ґрунтуються на різних методологіях, наборах даних та періодах. За оцінками Mordor Intelligence [13], глобальний ринок кібербезпеки сягнув 117 млрд євро в 2021 році і, за прогнозами, зросте до 195,9 млрд євро в 2026 році при річному темпі зростання 14,5% в 2021-2026 роках. Fortune Business Insights [12] прогнозує його зростання приблизно до 326 млрд євро у 2028 році за сукупного річного темпу зростання (CAGR) у 12,0%, тоді як Allied Market Research [14] підрахував, що глобальний ринок кібербезпеки оцінюватиметься у 272,6 млрд євро у 2027 році за середньорічного темпу зростання трохи нижче 10%. Momentum Cyber [15] оцінила десятикратне зростання щорічних глобальних інвестицій у кібербезпеку у період 2010-2019 років. Країни з кіберринками, що найбільш швидко ростуть, зосереджені в Азіатсько-Тихоокеанському регіоні (з очікуваним середньорічним темпом зростання 19,6%), при цьому Європа і Північна Америка характеризуються середніми темпами зростання (9,1% і 7,8% відповідно). Розвиток процесів цифровізації фінансових продуктів та послуг актуалізує ризик кіберзлочинності. Загроза з боку кіберзлочинців дедалі більше спрямовується як на самі фінансові установи, так і на клієнтів, яких вони обслуговують. Фінансовий сектор є одним із найбільш часто атакованих секторів, який відчуває потужний витік даних. Кількість розподілених атак відмови в обслуговуванні (DDoS) або атак на сервер, як правило, з метою зробити веб-сайт недоступним, збільшується, і вони стають дедалі більш цілеспрямованими [16]. І хоча здебільшого такі атаки все частіше орієнтуються на великі компанії, представники приватного сектору також виступають їхніми об'єктами. Соціальні витрати від кіберзлочинності значні. По-перше, існують прямі витрати від крадіжки грошей, наприклад, за допомогою фішингової атаки, коли довірливим користувачам пропонують підроблені сайти, які створюють кіберзлочинці. Такі сайти можуть повністю імітувати веб-сторінку,

наприклад, великого банку або соціальної мережі. Мета шахрайства - змусити користувача передати «ключі» від банківського рахунку або облікового запису в соціальній мережі в руки зловмисників. По-друге, існують непрямі витрати, оскільки фінансові установи повинні інвестувати в IT-безпеку. За оцінками, річні збитки від кіберзлочинів для світової економіки в 2020 році оцінюються в 5,5 трлн євро, що вдвічі більше, ніж у 2015 році [17]. За даними Європейської комісії, до двох третин європейських інтернет-користувачів стикалися з проблемами, пов'язаними з безпекою, і 60% почуваються нездатними захистити себе від кібератак [18]. Нарешті, існують соціальні витрати, коли фінансові послуги стають недоступними внаслідок такої діяльності, як DDoS-атаки. Багаторівневість встановлених взаємозв'язків між фінансовими установами та третіми сторонами ускладнює управління розповсюдженням внутрішньої інформації. Слід зазначити, що доступ до внутрішньої інформації мають різні організації, а відтак існує ризик її витоку у кожній ланці ланцюга (Див.Рис.1).

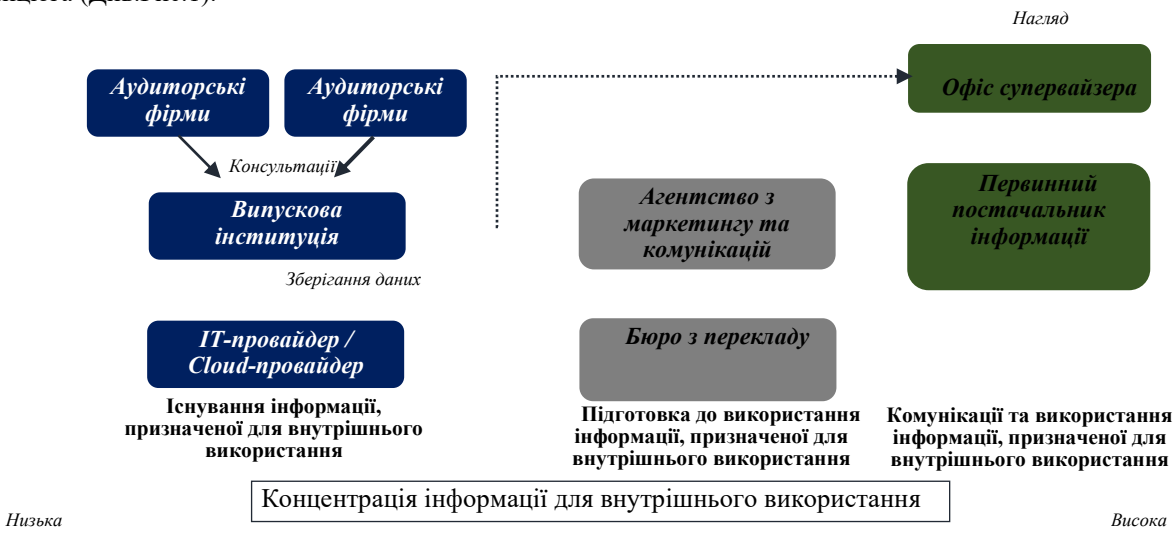

Рис. 1. Візуалізація ступеня доступу до інформації для внутрішнього використання різними учасниками інформаційного ланцюжка

Джерело: [19]

Наприклад, злочинці намагаються отримати доступ до медіа-агентств з метою завчасного ознайомлення зі змістом прес-релізів організацій. Цей ризик зростає разом із збільшенням кількості гравців у ланцюзі, таких як хмарні провайдери або постачальники IT. Аутсорсинг послуг, що здійснюється багатьма фінансовими установами, створює ризики концентрації для всього сектору. Якщо фінансові установи стануть залежними від обмеженої кількості постачальників основних програм, це може створити ризик неотримання послуги в наслідок відмови. Фінансові установи все частіше використовують послуги хмарних провайдерів для зберігання даних. Дохід від хмарних послуг зазнає експоненціального зростання, але є лише декілька гравців, що мають достатній потенціал для обслуговування великих установ. Як приклад, три найбільші хмарні провайдери (Amazon, Microsoft та Google) обслуговують понад 90% ринку. Такий розподіл ринку може збільшувати залежність від спроможності обмеженої кількості провайдерів протистояти кібератакам. Фінансові підприємства та аудиторські фірми виконують важливу роль у запобіганні використанню фінансової системи для фінансової злочинної діяльності. «Гейткіперська» роль фінансових установ полягає у здатності відсіювати недостовірну інформацію, попереджувати фрод та інші зловживання, нести відповідальність за неупередженість і достовірність інформації. Ця роль «гейткіперів», яку вимушено мають відігравати інститути колективного інвестування, інвестиційні фірми, аудиторські фірми та постачальники фінансових послуг, є важливою для боротьби з відмиванням грошей та фінансуванням тероризму, для контролю за недотриманням порушення санкційного режиму, запобігання шахрайства та фактів корупції. На Рис.2 наведено взуалізацію ймовірності того, що фінансові підприємства та аудиторські фірми ненавмисно будуть використані для злочинної діяльності.

Цифровізація збільшує ризик ненавмисної участі у фінансових злочинах, наприклад, через змішування кримінальних грошей із легальними доходами, які важко виявити [20]. Такі технологічні розробки, як технології блокчейн, криптовалюти та альтернативні платіжні системи (PSP), призводять до відмивання грошей у постійно зростаючих обсягах, що представляє собою нові виклики для фінансового сектору. Це вимагає високого ступеня пильності з боку фінансових установ, аудиторських фірм і наглядових органів, а також актуалізує зростаючі вимоги щодо управління операційними ризиками. PSP, які найчастіше виступають fintech-компаніями, дозволяють конвертувати валюту, отримувати платежі від клієнтів, виводити прибуток на банківський рахунок. Зокрема, спостерігається тенденція, коли фінансові установи запроваджують нові форми впливу за допомогою гейміфікації. Гейміфікація — це застосування ігрових прийомів і «ігрового мислення» в середовищі вибору споживачів, але поза традиційною сферою

комп'ютерних чи відеоігор. Приклади ігрових прийомів включають можливість заробляти бонуси та очки та грати з друзями та / або незнайомцями або проти них. Додавання цих елементів заохочує споживачів до продовження гри. Кількість геймерів у всьому світі оцінюється понад у 2 мільярда, а галузь кіберігор перевищила межу в 100 млрд дол США ще у 2017 році [21]. Гейміфікація активно впроваджується на фінансових ринках, наприклад, у фінансовій освіті, банківському секторі та інвестиційних послугах. Крім того, оцифрування фінансових послуг означає, що фінансові продукти та послуги стають дедалі доступнішими на низькопорогових платформах, таких як смартфони, завдяки чому споживачі можуть швидше приймати фінансові рішення. Гейміфікація може зробити особисті фінанси привабливішими для споживачів. Як правило, споживачі мало цікавляться фінансовими продуктами, такими як пенсії та страхування на випадок професійної втрати працездатності, що пов'язано із тим, що ці товари є складними за їхніми характеристиками. Через те, що наслідки прийнятих рішень стануть помітними лише в довгостроковій перспективі, споживачі схильні їх відкладати. Гейміфікація стає ефективним способом активізації споживачів та утримання їхньої уваги, оскільки це відповідає внутрішній мотивації людей вчитися, досягти певного статусу або отримати певний ступінь визнання. Гейміфікація стає інструментом зовнішньої мотивації людей у той момент, коли вводяться елементи перемоги. Додавання соціальних аспектів, таких як можливість спільної роботи, спілкування в чаті чи поєдинків з іншими геймерами, означає, що досвід стає більш приємним і що гравці можуть кинути виклик один одному, щоб продовжувати грати у грі та досягати цілей. Отже, гейміфікація може розширити знання споживачів про фінансові продукти та концепції через гру та заохотити їх до активної участі в управлінні своїми фінансами. При цьому наглядовим регуляторам слід брати до уваги, що нові методи впливу на поведінку споживачів фінансових послуг можуть також мати шкідливі або небажані ефекти (або побічні ефекти). Наприклад, гейміфікація може спричинити ризик звикання, оскільки споживачі втрачають контроль над своєю ігровою поведінкою. Введення ігрових елементів, таких як змагання та рівні статусу, крім того, може розмити межу між грою та реальністю. На відміну від звичайних комп'ютерних ігор, які також пов'язані з цим ризиком, ігрові елементи, що викликають звикання у фінансових продуктах, можуть призвести до істотних фінансових наслідків для споживачів, зокрема, сформувати заборгованість, коли споживачі зазнають невдачі або не можуть вчасно зупинити гру.

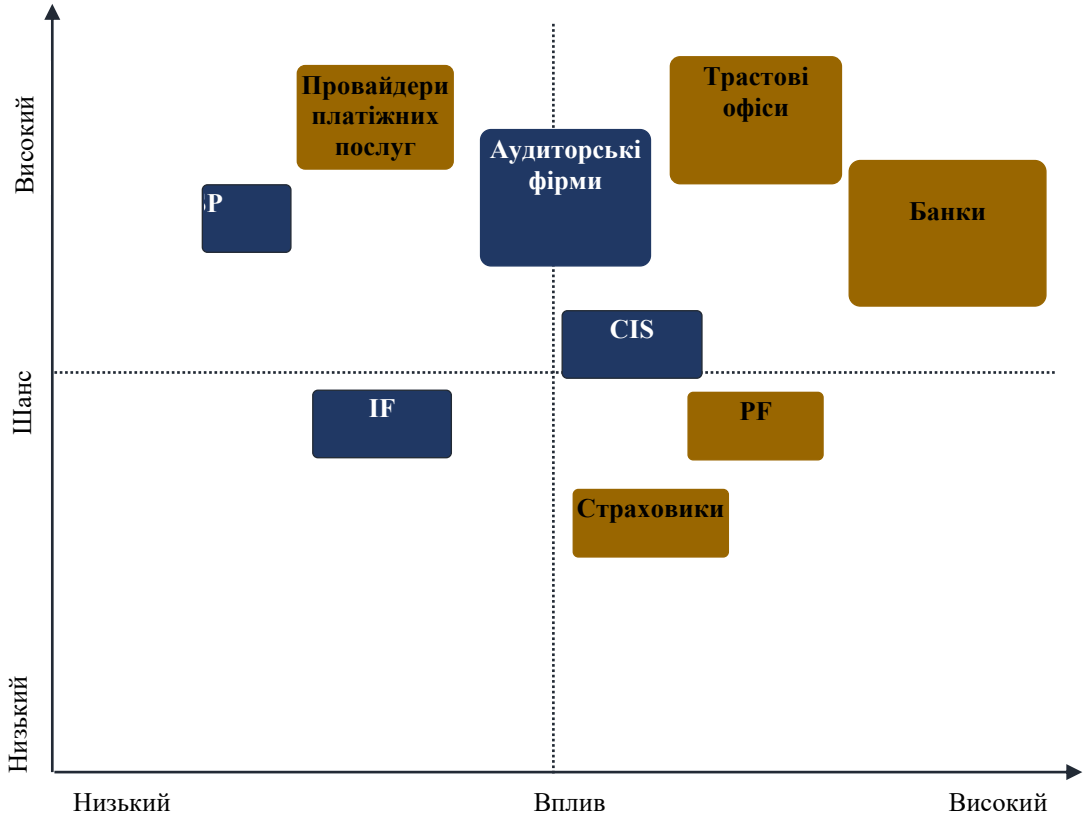

Рис. 2. Матриця ймовірності / впливу ненавмисного використання інформації для злочинної діяльності
Джерело: [19]
Примітка: розмір прямокутника показує відносну важливість гейткіперську роль установ
Скорочення: FSP — постачальники фінансових послуг, які виступають посередниками у страхуванні життя; IF — інвестиційні фонди; CIS — схеми колективних інвестицій; PF — пенсійні фонди.

Великі технологічні фірми, такі як Alibaba, Amazon, Facebook або Mercado Libre почали кредитувати постачальників на своїх торгових платформах. Цей новий вид кредиту вже набув певної актуальності і з огляду на зростання електронної комерції може посісти особливі позиції на міжнародному ринку позичкового капіталу. Зміни у фінансовому посередництві можуть суттєво вплинути на трансмісійні канали грошово-кредитної політики, що стане новим викликом для фінансових регуляторів і Центробанків, адже бізнес-модель Big Techs заснована на збиранні та використанні величезних масивів даних, але не для вирішення агентських проблем між кредиторами та позичальниками. Хоча кредитний скоринг, створений із використанням технологій машинного навчання та великих даних, і здатний визначати характеристики компаній із більшою точністю, ніж традиційні рейтинги кредитних бюро. Більше того, через мережеві ефекти та наявність високих витрат на перемикання між платформами, Big Tech можуть сприяти примусовому погашенню кредиту, просто погрожуючи вилученням зі своєї екосистеми у разі дефолту фірми. Це пояснює, чому великий технологічний кредит не корелює із вартістю нерухомості, але натомість сильно корелює з характерними для фірми характеристиками, такими як обсяги транзакцій на платформі електронної комерції Big Tech. У міру зростання частки великих технологічних кредитів грошово-кредитна політика менше впливатиме на пропозицію кредиту через ціни на активи (через традиційний «заставний канал», а більше через обмеження сумісності стимулів погашення в екосистемах великих технологій.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Посилення цифровізації глобальної економіки впливає на способи, в які банки виробляють і надають фінансові послуги своїм клієнтам, а також залучають Big Techs і FinTechs до цих процесів, і матиме революційні наслідки для існуючих фінансових установ і, особливо, традиційних банків. Остання хвиля цифровізації була спровокована прогресом у сфері телекомунікацій та інформаційних технологій. Існує ряд потенційних причин, через які великі технологічні компанії можуть нарощувати свою присутність на ринках фінансових послуг. Розширення пропозиції фінансових послуг може ще більше диверсифікувати джерела доходів, генерувати більше даних про витрати та заощадження, що допоможе їхньому основному бізнесу, та стимулювати взаємодію, серед іншого, полегшуючи проведення платежів на їхніх платформах. Розвиток «контекстних фінансів», в яких фінансові програми об'єднані в додаток або платформу, призначену для полегшення ділової активності, здійснюватиме самопосилюючий вплив на решту послуг: дані, зібрані про моделі заощаджень та витрат на вихідних ринках компаній та існуючі фінансові пропозиції, можуть вплинути на вибір майбутніх пропозицій фінансових послуг або компаній, які використовують таку модель. Наскільки активно зростатиме участь Big Techs на ринку фінансових послуг, і скільки послуг вони можуть зрештою запропонувати — залишається відкритим питанням, втім залежатиме від перспектив отриманням Big Techs і FinTechs статусу комерційних банків або статусу банку з повним обмеженим спектром послуг, що вимагатиме відповідного нагляду з боку регулюючих органів, які зацікавлені у протидії відмиванню грошей і тінізації глобальної економіки. Втім отримання статусу банку великими технологічними компаніями лише загострить їхню конкуренцію з класичними комерційними банками, що при цьому виступають споживачами хмарних послуг великих технологічних компаній.

Розвиток небанківського фінансового сектора може виявитись корисним з макропруденційної точки зору, оскільки він стимулюватиме розподіл ризиків у фінансовій системі. При цьому нішеві банківські бізнес-моделі, які вважаються стабільними і безпечними для банків, наражатимуться на конкуренцією зі сторони небанківських організацій. Крім того, фінансові ризики, в тому числі ризики ліквідності, іманентні надавачам послуг фінансового посередництва, можуть переміститися в ті сфери фінансової системи, які зазвичай не регулюються так прискіпливо, як банківський сектор. Окреслене свідчить, що цифровізація ринків капіталу і банківської діяльності зокрема формує запит на посилення наглядової функції фінансових регуляторів задля мінімізації тактичних і системних ризиків, протидії кіберризиків, а також проявів інформаційної асиметрії на ринку фінансових послуг, що надаються Big Techs і FinTechs.

Література

1. European Banking Authority. RISK ASSESSMENT OF THE EUROPEAN BANKING SYSTEM [Електронний ресурс] / European Banking Authority. – 2017. – Режим доступу: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2037825/4f9778cc-1ccd-4f65-9bc3-eb76971b9a4a/Risk%20Assessment%20Report%20-%20November%202017.pdf?retry=1

2. Herendy C. BIG BANKS AREN'T WAITING IDLY, DIGITAL BANKING IN THE NETHERLANDS – PART 2 [Електронний ресурс] / C. Herendy. – 2017. – Режим доступу: https://ergomania.eu/big-banks-arent-waiting-idly-digital-banking-in-the-netherlands-part-2/

3. PwC. Redrawing the Lines: FinTech's Growing Influence on Financial Services [Електронний ресурс] / PwC. – 2017. – Режим доступу: https://www.pwc.com/jg/en/issues/redrawing-the-linesfintechs-growing-influence-on-the-financial-services-2017.html.

4. Kulkarni T. Top U.S. Banks Are Investing Most in Personal Finance Fintechs [Електронний ресурс] / T. Kulkarni. – 2018. – Режим доступу: https://bankinnovation.net/2018/02/ top-u-s-banks-are- investing-most-in-personal-finance-fintechs/

5. Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks [Електронний ресурс] / G. Buchak, G. Matvos, T. Piskorski, A. Seru. – 2018. – Режим доступу: http://www.nber.org/papers/w23288.

6. МВФ. Fintech and Financial Services: Initial Considerations [Електронний ресурс] / МВФ. – 2017. – Режим доступу: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

7. KPMG.Regulation and supervision of fintech [Електронний ресурс] / KPMG. – 2019. – Режим доступу: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf

8. Boston Consulting Group. Global Wealth 2019 Reigniting Radical Growth [Електронний ресурс] / Boston Consulting Group. – 2019. – Режим доступу: https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf.

9. Baur-Yazbeck S. CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT. Challenges and potential solutions for financial inclusion [Електронний ресурс] / S. Baur-Yazbeck, J. Frickenstein, D. Medine. – 2019. – Режим доступу: https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf

10. IBM Security. X-Force Threat Intelligence Index 2022 [Електронний ресурс] / IBM Security. – 2022. – Режим доступу: https://www.ibm.com/downloads/cas/ADLMYLAZ.

11. State Bank Supervisors. CSBS National Survey of Community Banks 2021 [Електронний ресурс] / State Bank Supervisors. – 2021. – Режим доступу: https://www.communitybanking.org/~/media/files/publication/cb21publication_2021.pdf

12. Fortune Business Insights. Cyber security market size, share & COVID-19 impact analysis, by component (solution and services), by deployment type (cloud and on-premise), by enterprise size (small & medium enterprise and large enterprise), by industry (BFSI, IT and telecommunications, retail, healthcare, government, manufacturing, travel and transportation, energy and utilities and others) and region forecast, 2022–2029 [Електронний ресурс] / Fortune Business Insights. – 2022. – Режим доступу: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.

13. Mordor Intelligence. Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026) [Електронний ресурс] / Mordor Intelligence. – 2020. – Режим доступу: https://www.mordorintelligence.com/industry-reports/cyber-security-market

14. Allied Market Research. Cyber security market — Global opportunity analysis and industry forecast, 2020–2027 [Електронний ресурс] / Allied Market Research. – 2020. – Режим доступу: https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

15. Momentum Cyber. Cybersecurity Almanac 2020 [Електронний ресурс] / Momentum Cyber. – 2020. – Режим доступу: https://momentumcyber.com/cybersecurity-almanac-2020/

16. KSN Report: Ransomware in 2016-2017 [Електронний ресурс]. – 2017. – Режим доступу: https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/

17. Joint Research Centre. Cybersecurity — Our digital anchor: A European perspective [Електронний ресурс] / Joint Research Centre. – 2020. – Режим доступу: https://www.researchgate.net/publication/353138450_Cybersecurity_our_digital_anchor_a_European_perspective

18. European Commission. Digital Economy and Society Index (DESI) [Електронний ресурс] / European Commission. – 2020. – Режим доступу: https://digital-strategy.ec.europa.eu/en/library/digitaleconomy-and-society-index-desi-2020

19. AFM. The Dutch Authority for the Financial Markets [Електронний ресурс] / AFM. – Режим доступу: https://www.afm.nl/en/verslaglegging/jaarverslag

20. Phillips R. Group Subsidiaries, Tax Minimization and Offshore Financial Centres: Mapping Organizational Structures to Establish the “in-betweener” Advantage / R. Phillips, H. Petersen, R. Palan // Journal of International Business Policy. – 2021. – Vol. 4. – P. 286–307.

21. Newzoo. Newzoo Global Games Market Report 2017 [Електронний ресурс] / Newzoo. – 2017. – Режим доступу: https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2017-light-version

References

1. European Banking Authority. RISK ASSESSMENT OF THE EUROPEAN BANKING SYSTEM [Elektronnyj resurs] / European Banking Authority. – 2017. – Rezhim dostupa: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2037825/4f9778cc-1ccd-4f65-9bc3-eb76971b9a4a/Risk%20Assessment%20Report%20-%20November%202017.pdf?retry=1

2. Herendy C. BIG BANKS AREN’T WAITING IDLY, DIGITAL BANKING IN THE NETHERLANDS – PART 2 [Elektronnyj resurs] / C. Herendy. – 2017. – Rezhim dostupa: https://ergomania.eu/big-banks-arent-waiting-idly-digital-banking-in-the-netherlands-part-2/

3. PwC. Redrawing the Lines: FinTech’s Growing Influence on Financial Services [Elektronnyj resurs] / PwC. – 2017. – Rezhim dostupa: https://www.pwc.com/jg/en/issues/redrawing-the-linesfintechs-growing-influence-on-the-financial-services-2017.html.

4. Kulkarni T. Top U.S. Banks Are Investing Most in Personal Finance Fintechs [Elektronnyj resurs] / T. Kulkarni. – 2018. – Rezhim dostupa: https://bankinnovation.net/2018/02/ top-u-s-banks-are- investing-most-in-personal-finance-fintechs/

5. Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks [Elektronnyj resurs] / G. Buchak, G. Matvos, T. Piskorski, A. Seru. – 2018. – Rezhim dostupa: http://www.nber.org/papers/w23288.
6. МВФ. Fintech and Financial Services: Initial Considerations [Elektronnyj resurs] / МВФ. – 2017. – Rezhim dostupa: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985
7. KPMG.Regulation and supervision of fintech [Elektronnyj resurs] / KPMG. – 2019. – Rezhim dostupa: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf
8. Boston Consulting Group. Global Wealth 2019 Reigniting Radical Growth [Elektronnyj resurs] / Boston Consulting Group. – 2019. – Rezhim dostupa: https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf.
9. Baur-Yazbeck S. CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT. Challenges and potential solutions for financial inclusion [Elektronnyj resurs] / S. Baur-Yazbeck, J. Frickenstein, D. Medine. – 2019. – Rezhim dostupa: https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf
10. IBM Security. X-Force Threat Intelligence Index 2022 [Elektronnyj resurs] / IBM Security. – 2022. – Rezhim dostupa: https://www.ibm.com/downloads/cas/ADLMYLAZ.
11. State Bank Supervisors. CSBS National Survey of Community Banks 2021 [Elektronnyj resurs] / State Bank Supervisors. – 2021. – Rezhim dostupa: https://www.communitybanking.org/~/media/files/publication/cb21publication_2021.pdf
12. Fortune Business Insights. Cyber security market size, share & COVID-19 impact analysis, by component (solution and services), by deployment type (cloud and on-premise), by enterprise size (small & medium enterprise and large enterprise), by industry (BFSI, IT and telecommunications, retail, healthcare, government, manufacturing, travel and transportation, energy and utilities and others) and region forecast, 2022–2029 [Elektronnyj resurs] / Fortune Business Insights. – 2022. – Rezhim dostupa: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.
13. Mordor Intelligence. Global cybersecurity market — Growth, trends, COVID-19 impact, and forecasts (2021–2026) [Elektronnyj resurs] / Mordor Intelligence. – 2020. – Rezhim dostupa: https://www.mordorintelligence.com/industry-reports/cyber-security-market
14. Allied Market Research. Cyber security market — Global opportunity analysis and industry forecast, 2020–2027 [Elektronnyj resurs] / Allied Market Research. – 2020. – Rezhim dostupa: https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf
15. Momentum Cyber. Cybersecurity Almanac 2020 [Elektronnyj resurs] / Momentum Cyber. – 2020. – Rezhim dostupa: https://momentumcyber.com/cybersecurity-almanac-2020/
16. KSN Report: Ransomware in 2016-2017 [Elektronnyj resurs]. – 2017. – Rezhim dostupa: https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/
17. Joint Research Centre. Cybersecurity — Our digital anchor: A European perspective [Elektronnyj resurs] / Joint Research Centre. – 2020. – Rezhim dostupa: https://www.researchgate.net/publication/353138450_Cybersecurity_our_digital_anchor_a_European_perspective
18. European Commission. Digital Economy and Society Index (DESI) [Elektronnyj resurs] / European Commission. – 2020. – Rezhim dostupa: https://digital-strategy.ec.europa.eu/en/library/digitaleconomy-and-society-index-desi-2020
19. AFM. The Dutch Authority for the Financial Markets [Elektronnyj resurs] / AFM. – 2020. – Rezhim dostupa: https://www.afm.nl/en/verslaglegging/jaarverslag
20. Phillips R. Group Subsidiaries, Tax Minimization and Offshore Financial Centres: Mapping Organizational Structures to Establish the “in-betweener” Advantage / R. Phillips, H. Petersen, R. Palan // Journal of International Business Policy. – 2021. – Vol. 4. – P. 286–307.
21. Newzoo. Newzoo Global Games Market Report 2017 [Elektronnyj resurs] / Newzoo. – 2017. – Rezhim dostupa: https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2017-light-version