УДК 336.7

https://doi.org/10.52058/3041-1254-2025-12(22)-1462-1474

Турський Олександр Віталійович аспірант ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», https://orcid.org/0009-0009-2092-778X

ІНФОРМАЦІЙНА БЕЗПЕКА ФІНАНСОВИХ УСТАНОВ У СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ: ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ

Анотація. Стаття присвячена дослідженню організаційно-правових засад забезпечення інформаційної безпеки фінансових установ у системі державного управління в умовах цифровізації публічних послуг, зростання кіберзагроз та підвищеної чутливості процесів обігу фінансових даних. Акцентовано, що фінансовий сектор одночасно виконує функції критичної інфраструктури та інструменту реалізації соціальної політики, а тому стійкість його інформаційних систем прямо впливає на безперервність платежів, захист персональних даних і довіру до державних інститутів.

Досліджено нормативно-інституційні підходи до державного регулювання кіберзахисту фінансових установ, зокрема через механізми нагляду, комплаєнсу, стандартизації, управління ризиками та координації між суб'єктами безпеки. Проаналізовано взаємодію регулятора, правоохоронних органів, спеціальних служб, органів виконавчої влади та учасників ринку у площині обміну інформацією про інциденти, реагування та відновлення, а також визначення відповідальності за порушення вимог безпеки.

Обґрунтовано необхідність інтеграції організаційних і правових інструментів у єдину модель публічного управління, що передбачає ризик-орієнтований підхід, обов'язковість процедур управління інцидентами, аудитів і тестування стійкості, регламентацію доступів та захист доказової бази у випадку кібератак. Доведено доцільність посилення регуляторних вимог до ланцюгів постачання IT-послуг, а також уніфікації вимог до реєстрів, платіжної інфраструктури та каналів електронної взаємодії, які забезпечують соціальні виплати.

Виявлено ключові проблеми практичної реалізації державної політики у сфері інформаційної безпеки фінансових установ: фрагментованість повноважень, нерівномірність спроможностей суб'єктів ринку, дефіцит кадрів, недостатня стандартизація процесів обміну даними про інциденти та ризики витоку персональної інформації.

Ключові слова: інформаційна безпека, фінансові установи, державне управління, кібербезпека, організаційно-правові засади, регулювання, комплаєнс, управління ризиками, критична інфраструктура, соціальні виплати.

Turskyi Oleksandr Vitaliiovych postgraduate student at PJSC “Higher Educational Institution ”Interregional Academy of Personnel Management", https://orcid.org/0009-0009-2092-778X

INFORMATION SECURITY OF FINANCIAL INSTITUTIONS IN THE SYSTEM OF PUBLIC ADMINISTRATION: ORGANIZATIONAL AND LEGAL FOUNDATIONS

Abstract. The article is devoted to studying the organizational and legal foundations for ensuring information security of financial institutions within the system of public administration under conditions of digitalization of public services, the growth of cyber threats, and the increased sensitivity of financial data circulation processes. It is emphasized that the financial sector simultaneously performs the functions of critical infrastructure and an instrument for implementing social policy; therefore, the resilience of its information systems directly affects the continuity of payments, the protection of personal data, and trust in public institutions.

The study examines regulatory and institutional approaches to state regulation of cybersecurity in financial institutions, in particular through mechanisms of supervision, compliance, standardization, risk management, and coordination among security stakeholders. The interaction between the regulator, law enforcement bodies, special services, executive authorities, and market participants is analyzed in terms of information exchange on incidents, response and recovery, as well as the determination of liability for violations of security requirements.

The necessity of integrating organizational and legal instruments into a unified model of public administration is substantiated; this model implies a risk-based approach, mandatory incident management procedures, audits and resilience testing, access regulation, and protection of the evidentiary base in the event of cyberattacks. The expediency of strengthening regulatory requirements for IT supply chains is argued, along with the unification of requirements for registers, payment infrastructure, and electronic interaction channels that ensure social payments.

Key practical implementation problems of state policy in the field of information security of financial institutions are identified, including fragmented mandates, uneven capacities across market participants, a shortage of qualified personnel, insufficient standardization of processes for sharing incident and risk information, and risks of personal data leakage.

Keywords: information security, financial institutions, public administration, cybersecurity, organizational and legal foundations, regulation, compliance, risk management, critical infrastructure, social payments.

Постановка проблеми. Цифровізація фінансових послуг і масштабне впровадження електронних сервісів у взаємодії держави, фінансових установ та громадян сформували новий рівень залежності соціальної сфери від стійкості платіжної інфраструктури, державних реєстрів і каналів обміну даними. За цих умов інформаційна безпека фінансових установ перестає бути суто корпоративним завданням і набуває ознак публічного інтересу, оскільки збої, витоки даних або кібератаки безпосередньо впливають на безперервність соціальних виплат, доступ населення до коштів, захист персональних даних та довіру до органів державної влади. Водночас зростання складності загроз, включно з атаками на ланцюги постачання IT-послуг, фішинговими кампаніями, компрометацією облікових записів, а також гібридними впливами в умовах воєнних ризиків, актуалізує потребу у чіткій, узгодженій та підзвітній системі державного управління кіберзахистом фінансового сектору.

Аналіз останніх досліджень і публікацій. Проблематика інформаційної безпеки фінансових установ розвивається на перетині юридичної науки, публічного управління та прикладної кібербезпеки: у фокусі перебувають питання нормативного забезпечення, інституційної координації, комплаєнсу та управління кіберризиками, а також узгодження вимог до стійкості критичних сервісів і платіжної інфраструктури. У вітчизняному дискурсі помітними є праці, що аналізують правове регулювання інформаційної безпеки та функціонування публічного управління у цій сфері, включно з підходами до захисту критичної інфраструктури.

Безпосередньо цю тематику в останніх роботах досліджували І. Сопілко, Л. Рапацька, О. Урсоль, Г. Кришталь, С. М. Козанчин, С. Р. Buttigieg, D. Clausmeier, A. Cojocaru. При цьому, попри наявність значної кількості напрацювань, додаткового обґрунтування потребує саме організаційно-правова «зв'язка» у системі державного управління, що має забезпечувати єдині правила взаємодії регулятора, фінансових установ і суміжних суб'єктів безпеки, зокрема в частині обміну даними про інциденти, вимог до стійкості та відповідальності за порушення режимів захисту.

Метою дослідження є комплексне обґрунтування організаційно-правових засад забезпечення інформаційної безпеки фінансових установ у системі державного управління та визначення пріоритетних напрямів удосконалення регуляторних і координаційних механізмів для підвищення кіберстійкості, захисту даних і безперервності соціально значущих фінансових сервісів.

Виклад основного матеріалу. Інформаційна безпека фінансових установ у системі державного управління на сучасному етапі постає не як допоміжний технічний напрям, а як ключова умова безперервності соціально значущих сервісів, стабільності платіжної інфраструктури та легітимності державної політики у сфері фінансів і соціального захисту. Масштаб цифрових операцій в Україні демонструє, що навіть короткострокові збої або компрометація

інформаційних систем здатні набувати суспільного резонансу та породжувати вторинні ризики: каскадні затримки виплат, дезінформаційні хвилі, панічні настрої, ажіотаж на готівку, конфлікти між сторонами у договірних та адміністративних правовідносинах. За даними Національного банку України, протягом 2024 року операції з платіжними картками, емітованими українськими банками та фінансовими установами, сягнули 8 654,4 млн транзакцій на суму 6 577,4 млрд грн, причому більшість операцій була безготівковою: 8 184,8 млн безготівкових транзакцій на суму 4 243,5 млрд грн, а частка безготівкових операцій за кількістю піднялася до 94,6 відсотка, що засвідчує високий рівень залежності населення та держави від стабільної роботи цифрових платіжних каналів [1]. У такій конфігурації державне управління не може обмежуватися загальними деклараціями про кіберзахист, оскільки фактичний контур державних функцій у соціальній сфері, освіті, медицині, підтримці вразливих груп та післявоєнному відновленні дедалі частіше реалізується через фінансові інститути як провідників платежів, ідентифікації, верифікації та обміну даними між реєстрами. Фактично фінансові установи стають вузловими точками, де концентруються потоки персональних даних, даних про доходи та статуси, платіжні реквізити, інформація про соціальну допомогу, а також технічні журнали подій, що формують доказову базу у випадку інцидентів та подальших процесуальних дій.

Особлива увага до організаційно-правових засад інформаційної безпеки фінансових установ зумовлена тим, що держава виступає одночасно й регулятором, і великим замовником фінансових послуг, і гарантом соціальних виплат, які часто здійснюються через банківські рахунки, карткові продукти, платіжні сервіси та інші інструменти фінансового ринку. Соціальні виплати є не просто бюджетною статтею, а інструментом забезпечення соціальної стабільності та реалізації конституційних гарантій, а тому їх доступність і своєчасність мають ознаки публічного інтересу та є предметом підвищеної уваги суспільства. Міністерство фінансів України повідомляло, що у 2024 році соціальні виплати були профінансовані у повному обсязі на суму 447,9 млрд грн, що відображає значний масштаб фінансових потоків, для яких критичними є цілісність даних, автентичність платіжних доручень, захист каналів дистанційного обслуговування, надійність інтеграцій з державними реєстрами та стійкість процесів верифікації отримувачів [2]. Якщо перенести ці параметри на площину державного управління, стає очевидним, що будь-який системний інцидент у фінансовому секторі потенційно перетворюється на інцидент у соціальній сфері, оскільки порушує доступ громадян до ресурсів існування, провокує зростання скарг, збільшує навантаження на органи влади, породжує спори між учасниками правовідносин та ускладнює доведення фактів у частині нарахувань, списань і повернень. У свою чергу, цифровізація соціальних послуг породжує нові адміністративно-правові виклики: необхідність регламентувати обмін даними,

визначати відповідальних за якість і актуальність відомостей, встановлювати порядок досудового розгляду справ у випадку помилкових списань чи блокувань, а також забезпечувати стандарти доказування для ситуацій, коли предметом спору стають електронні записи, журнали подій або результати автоматизованих перевірок.

Загрозовий ландшафт для фінансових установ в Україні характеризується поєднанням масових кіберзлочинних практик і цілеспрямованих атак у контексті гібридного протиборства, де фінансовий сектор розглядається як приваблива ціль через доступ до коштів, персональних даних і можливість досягнення суспільно-політичного ефекту. Рівень інцидентності підтверджується статистикою національних кіберінституцій: за повідомленням профільного державного ресурсу у сфері кіберзахисту, CERT-UA опрацювала 4 315 кіберінцидентів протягом 2024 року, що свідчить про високу інтенсивність подій та потребу в стандартизованому циклі реагування на рівні держави й ринку [3]. Водночас кількісний показник інцидентів має розглядатися не як абстрактна цифра, а як індикатор навантаження на систему управління: за кожним інцидентом стоять управлінські рішення щодо ізоляції сегментів мережі, відновлення резервних копій, комунікацій із клієнтами, повідомлення регулятора, взаємодії з правоохоронними органами, фіксації цифрових доказів і мінімізації шкоди. Практика показує, що найболючішими для фінансових установ є інциденти, які зачіпають доступність і довіру: від зупинки дистанційних каналів обслуговування та платіжних шлюзів до компрометації облікових записів клієнтів через фішинг, соціальну інженерію або повторне використання паролів, а також до атак на ланцюги постачання, коли ураження виникає не в самій установі, а в її підрядника з ІТ-послуг. Для державного управління це означає, що регуляторні акценти мають зміщуватися від формального контролю документів до перевірки реальної спроможності установ виконувати критичні функції в умовах інциденту, зокрема підтримувати безперервність соціальних виплат, коректність обліку та відновлюваність даних, що в подальшому формують доказову базу для захисту прав отримувачів і врегулювання спорів між сторонами.

Організаційно-правові засади інформаційної безпеки фінансових установ у системі державного управління проявляються передусім через модель регуляторного впливу, де Національний банк України як регулятор і наглядовий орган встановлює вимоги до управління ризиками, безпеки інформаційних систем, процедур реагування, контролю третіх сторін та внутрішнього комплаєнсу. Показовим є те, що наприкінці 2025 року регулятор посилив нормативний каркас для небанківського сегмента: Національний банк України повідомив про набрання чинності з 13 грудня 2025 року постанови Правління НБУ від 9 грудня 2025 року № 143, якою затверджено Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг, а також визначено перехідний період для приведення діяльності у

відповідність до нових вимог протягом року [4]. Значення цього акту виходить за межі суто технічних вимог, оскільки він фактично задає рамку організаційної відповідальності: визначення ролей і повноважень у сфері безпеки, вимоги до політик, до управління інцидентами, до контролю доступів, до навчання персоналу, до моніторингу та до взаємодії з підрядниками. У площині державного управління це свідчить про перехід до моделі, де інформаційна безпека розглядається як елемент системи управління установою, підзвітний керівним органам і інтегрований у загальні процеси ризик-менеджменту, а не як ізольована функція ІТ-підрозділу. Практична імплементація таких вимог впливає на захист прав отримувачів соціальної допомоги, оскільки саме небанківські надавачі фінпослуг дедалі активніше залучаються до платіжної інфраструктури, цифрових гаманців, сервісів переказу та інших рішень, що можуть використовуватися у державних програмах підтримки населення.

Базовим елементом правового підґрунтя державної політики у сфері інформаційної безпеки є національне законодавство про кібербезпеку, яке визначає принципи, суб'єктний склад, координаційні механізми та загальні засади захисту критично важливих інформаційних ресурсів. Закон України про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року № 2163-VIII закріплює фундаментальні поняття та підходи до розбудови національної системи кібербезпеки, що важливо для фінансових установ як учасників середовища, де інциденти можуть набувати міжсекторного характеру та вимагати міжвідомчої взаємодії [5]. Організаційно-правова цінність такого закону полягає в тому, що він задає рамку для координації, обміну інформацією, визначення ролей і відповідальності, а отже створює основу для побудови процедур, які у випадку інциденту забезпечують не лише технічне відновлення, а й правову визначеність: хто повідомляє, кому повідомляє, у які строки, за якими каналами, які дані є допустимими до передавання, як забезпечується режим доступу та конфіденційність. Для фінансових установ це означає, що їх внутрішні політики мають узгоджуватися з публічними вимогами й очікуваннями держави, а також із необхідністю збереження доказів, придатних для подальшого використання у кримінальному провадженні, цивільних справах або адміністративних процедурах, коли сторони спору доводять факт несанкціонованих транзакцій, підміни реквізитів або компрометації облікових даних.

Невід'ємною складовою організаційно-правових засад є також правове регулювання захисту критичної інфраструктури, оскільки фінансовий сектор і платіжна інфраструктура за своєю природою здатні генерувати системні ризики, а їх стійкість має значення для національної безпеки та соціальної стабільності. Закон України про критичну інфраструктуру від 16 листопада 2021 року № 1882-IX визначає правові та організаційні засади функціонування національної системи захисту критичної інфраструктури, що створює підстави для класифікації об'єктів, визначення вимог до їх захисту, планування заходів безпеки та

координації суб'єктів [6]. У контексті фінансових установ це дає змогу застосовувати підхід, за яким пріоритетом стає не рівномірне посилення всіх систем, а забезпечення стійкості критичних функцій: виплат і переказів, обробки транзакцій, доступу до рахунків, маршрутизації платежів, роботи контакт-центрів та механізмів відновлення. Такий підхід особливо важливий для державних програм соціальної підтримки, оскільки навіть часткова деградація сервісів може порушити принцип адресності й своєчасності, а також спровокувати хвилю звернень, скарг і спорів. З управлінської точки зору, застосування критичної інфраструктурної логіки означає необхідність встановлювати вимірювані цілі стійкості, часові параметри відновлення, вимоги до резервування, сценарії реагування та взаємодії з державними структурами, у тому числі щодо інформаційного обміну під час криз.

Ключовим правовим виміром інформаційної безпеки фінансових установ є захист персональних даних, оскільки фінансові транзакції та соціальні виплати нерозривно пов'язані з обробкою ідентифікаційної інформації, контактних даних, відомостей про доходи, статуси та чутливих категорій, які в сукупності формують профілі громадян. Закон України про захист персональних даних від 1 червня 2010 року № 2297-VI регулює правовідносини, пов'язані із захистом і обробкою персональних даних, і спрямований на забезпечення основоположних прав і свобод людини, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних [7]. Для фінансових установ у системі державного управління це означає, що інформаційна безпека повинна проєктуватися як режим правомірної обробки: мінімізація даних, визначеність мети, легітимність підстав, контроль доступів, прозорість процедур, а також обмеження щодо передавання даних третім особам, у тому числі підрядникам і технологічним операторам. У практичному вимірі це вимагає від держави та регулятора запровадження вимог не лише до технічних засобів захисту, а й до процесів: ведення реєстрів доступів, журналювання дій, сегментації даних, впровадження принципу найменших привілеїв, а також процедур реагування на інциденти витоку, де центральним стає питання доведення фактів, обсягу шкоди та належного повідомлення осіб, чиї дані були скомпрометовані. Саме тут перетинаються інформаційна безпека й справедливе судочинство, оскільки якість доказової бази та процесуальні аспекти фіксації цифрових слідів визначають можливість ефективного захисту прав громадян у суді або під час досудового розгляду справ.

Важливий шар організаційно-правових засад формує також спеціальне законодавство про платіжні послуги, яке описує логіку функціонування платіжного ринку, визначає категорії надавачів, засади нагляду й оверсайту платіжної інфраструктури, а отже безпосередньо впливає на вимоги до безпеки транзакцій та каналів взаємодії. Закон України про платіжні послуги від 30 червня 2021 року № 1591-IX визначає загальний порядок здійснення платіжних операцій, засади

функціонування платіжних систем, а також загальні процедури нагляду за діяльністю надавачів платіжних послуг і оверсайту платіжної інфраструктури [8]. Для цілей інформаційної безпеки це означає, що держава має правові інструменти, щоб вимагати належного рівня захисту платіжних операцій, встановлювати правила ідентифікації та автентифікації, регламентувати обмін інформацією між учасниками ринку, а також визначати вимоги до технологічних операторів, які забезпечують процесинг і маршрутизацію транзакцій. У контексті соціальних виплат це набуває особливого значення, бо значна частина виплат реалізується через платіжні інструменти та інфраструктуру, де навіть незначні вразливості можуть призводити до шахрайських списань, підміни реквізитів або блокування доступу до коштів. Відповідно, організаційно-правова модель має включати механізми превенції шахрайства, моніторинг аномалій, узгоджені правила повернення коштів, а також процедури взаємодії між регулятором, фінансовою установою та правоохоронними органами з урахуванням вимог до доказів і доказової бази.

Євроінтеграційний вимір державного управління вимагає узгодження підходів України до інформаційної безпеки фінансового сектору з регуляторними стандартами ЄС, які посилюють вимоги до цифрової операційної стійкості, інцидент-менеджменту, управління ризиками ІКТ та контролю третіх сторін. На рівні Європейського Союзу показовим є ухвалення та впровадження Digital Operational Resilience Act, який установлює комплексні правила цифрової операційної стійкості для фінансового сектору і застосовується з 17 січня 2025 року, що є важливим орієнтиром для державної політики в Україні з огляду на інтеграційні процеси та потребу взаємосумісності підходів [9]. Концептуально DORA важлива тим, що переносить акцент із розрізнених вимог на єдину управлінську рамку: управління ризиками ІКТ як частина корпоративного управління, стандартизовані процедури повідомлення про інциденти, систематичне тестування стійкості, управління ризиками від сторонніх провайдерів ІКТ і наглядова координація. Для України це означає практичну доцільність формувати такі організаційно-правові рішення, які забезпечують мінімальний однаковий рівень вимог для ключових гравців, прозорі правила взаємодії та порівнювані метрики стійкості, що полегшують нагляд і контроль, а також підвищують довіру до фінансового сектору як до інструмента реалізації соціальної політики.

Економічна аргументація інформаційної безпеки у фінансовому секторі посилює вимоги до державного управління, оскільки кіберінциденти мають не лише прямі технічні наслідки, а й вимірювані фінансові втрати, репутаційні збитки, витрати на відновлення, юридичні ризики та потенційні компенсації. За даними IBM Cost of a Data Breach 2024, середня глобальна вартість витоку даних досягла 4,88 млн дол. США, а для фінансової галузі середні витрати є вищими і становлять 6,08 млн дол. США, що демонструє об’єктивну економічну вагу

інцидентів і потребу в системних інвестиціях у стійкість [10]. У площині державного управління це означає, що регулювання має бути спрямоване не тільки на формальне виконання процедур, а й на досягнення результату: зниження частоти інцидентів, скорочення часу виявлення й локалізації, забезпечення відновлюваності даних, мінімізацію втрат для клієнтів та державних програм. Водночас економічний аспект прямо пов'язаний з правовими наслідками: що більша шкода, то частіше виникають спори між сторонами, вимоги відшкодування, питання відповідальності за недбалість або порушення вимог безпеки, а також необхідність формувати переконливу доказову базу щодо причин інциденту, факту компрометації та ланцюга подій.

Подальше розкриття організаційно-правових засад доцільно здійснювати через логіку управлінського циклу, який у фінансових установах має бути синхронізований із функціями держави як регулятора та гаранта суспільно значущих виплат. На стратегічному рівні ключовим є корпоративне управління безпекою: визначення апетиту до ризику, затвердження політики інформаційної безпеки, розподіл ролей між наглядовими органами, правлінням і функціями контролю, встановлення вимог до звітності, а також інтеграція інформаційної безпеки у систему внутрішнього контролю й комплаєнсу. Для державного управління важливо, щоб така модель не була декларативною, а підтверджувалася перевірюваними практиками: регулярними аудитами, тестуванням планів реагування, навчанням персоналу та перевіркою готовності до інцидентів. Саме через це наглядові механізми мають оцінювати не тільки наявність документів, а й реальне функціонування процесів, включно з тим, як установа забезпечує захист соціальних виплат як критичного сервісу, як вона документує інциденти, як формує докази для подальшого розгляду справ і як взаємодіє з органами влади у кризових ситуаціях.

На операційному рівні організаційно-правові засади проявляються через стандартизацію процесів управління ризиками та інцидентами. Ризик-орієнтований підхід передбачає ідентифікацію критичних активів і процесів, класифікацію даних, моделювання загроз, оцінку вразливостей, визначення контрольних заходів і регулярне переоцінювання ризиків. Для фінансових установ критичними є процесинг, системи дистанційного банкінгу, платіжні шлюзи, інтеграції з державними реєстрами, контакт-центри та системи обліку, що забезпечують нарахування й проведення виплат. Інцидент-менеджмент, своєю чергою, має включати чіткі процедури: виявлення, реєстрацію, класифікацію, локалізацію, усунення, відновлення, післяінцидентний аналіз і управлінські висновки. Для держави ключове питання полягає в тому, щоб ці процедури були порівнюваними між установами та забезпечували прогнозованість: визначені строки повідомлення, стандарти мінімального набору даних про інцидент, єдині підходи до взаємодії з CERT-UA, регулятором та правоохоронними органами, а також вимоги до збереження цифрових доказів, які можуть бути використані під час досудового розгляду справ і в суді.

Забезпечення доказової бази у випадку інцидентів є одним із найбільш недооцінених елементів організаційно-правових засад, хоча саме він визначає спроможність сторін обґрунтувати позицію у спорі, довести обставини несанкціонованих транзакцій та забезпечити справедливе судочинство. У контексті фінансових установ це означає необхідність регламентувати: політику журналювання, правила збереження логів, синхронізацію часу, процедури зняття копій, ланцюг зберігання доказів, контроль доступу до матеріалів інциденту, а також порядок взаємодії між підрозділами безпеки, юридичною службою та комплаєнсом. Для державного управління важливо встановити мінімальні стандарти, які забезпечують придатність доказів незалежно від технологічної платформи установи, бо інакше у судовому процесі або під час розгляду скарги постає проблема допустимості й достовірності електронних доказів, а також проблема того, чи була установа належно організована для запобігання та фіксації порушень. У соціально чутливих випадках, коли предметом спору є доступ громадянина до соціальних виплат, саме якісна доказова база дозволяє відновити справедливість, встановити факт компрометації або технічної помилки та ухвалити обґрунтоване рішення.

Управління доступами та ідентифікацією користувачів у фінансовому секторі має розглядатися як елемент публічної безпеки, оскільки компрометація облікових записів клієнтів або співробітників здатна призводити до незаконних переказів, підміни реквізитів соціальних виплат і масових звернень громадян. Організаційно-правова модель тут має поєднувати вимоги до багатофакторної автентифікації, управління привілеями, сегментації доступу, контролю підозрілих входів, а також політик щодо мобільних пристроїв, віддаленої роботи та використання хмарних сервісів. У площині державного управління це означає потребу в узгодженні вимог до електронної ідентифікації, до взаємодії з державними реєстрами, до процедур верифікації отримувачів і до механізмів запобігання шахрайству, включно з інформаційним обміном про типові схеми. Практичні приклади свідчать, що масові атаки часто використовують комбіновані методи: соціальну інженерію, підміну SIM-карт, компрометацію електронної пошти та викрадення токенів сесій, а тому регуляторні вимоги мають включати не тільки технічні заходи, а й обов’язкове навчання персоналу та клієнтські комунікації, спрямовані на зниження успішності таких атак.

Окремий пласт становить управління третімі сторонами та ланцюгами постачання, оскільки фінансові установи активно залежать від процесингових центрів, хмарних провайдерів, постачальників програмного забезпечення, аутсорсингових контакт-центрів і сервісних компаній. Організаційно-правові засади вимагають, щоб договори з такими контрагентами містили вимоги до безпеки, права на аудит, правила повідомлення про інциденти, обмеження щодо субпідрядників, вимоги до локалізації даних і параметрів відновлення. Для державного управління це означає, що регулювання повинно враховувати не

лише власне фінансові установи, а й екосистему постачальників, оскільки слабка ланка в ланцюгу постачання часто стає точкою входу для атаки. Додатковий правовий аспект полягає в тому, що під час інциденту можуть виникати спори про відповідальність: між фінансовою установою та постачальником, між установою та клієнтом, між учасниками платіжної системи.

Питання безперервності діяльності та відновлення після інцидентів є серцевиною організаційно-правових засад, якщо фінансові установи розглядаються як елементи виконання державою соціальних зобов'язань. У практичному вимірі необхідно встановлювати параметри безперервності для критичних сервісів, зокрема для виплат, які мають соціальне значення, визначати допустимі часові межі простою, вимоги до резервних копій і планів відновлення, сценарії роботи у деградованому режимі, а також порядок пріоритизації відновлюваних функцій. Для державного управління важливо, щоб ці параметри не були внутрішньою справою установи, а узгоджувалися з суспільними потребами: наприклад, щоб у періоди пікових соціальних виплат або реалізації програм підтримки населення установи мали підвищений режим моніторингу, посилені процедури контролю транзакцій і готовність до швидкого відновлення.

Таким чином, організаційно-правові засади інформаційної безпеки фінансових установ у системі державного управління доцільно розуміти як багаторівневу конструкцію, що поєднує законодавчі вимоги, регуляторні стандарти, наглядові процедури, внутрішні політики та управлінські практики установ, а також механізми координації, реагування й доказування. Їх ефективність вимірюється не кількістю документів, а здатністю забезпечити безперервність соціально значущих сервісів, захист персональних даних, стійкість платіжної інфраструктури, передбачуваність відповідальності та спроможність формувати належну доказову базу для захисту прав громадян і законних інтересів сторін у разі інцидентів. Умови воєнних і гібридних загроз, зростання масштабів безготівкових операцій та значні обсяги соціальних виплат роблять цю проблематику системною, а отже вимагають подальшого розвитку інтегрованих підходів, що поєднують публічне управління, право, кібербезпеку, нагляд і практики операційної стійкості.

Висновки. Проведене дослідження дозволяє стверджувати, що інформаційна безпека фінансових установ у системі державного управління є не лише напрямом технічного захисту, а комплексною організаційно-правовою конструкцією, від якої залежить безперервність соціально значущих платежів, стабільність платіжної інфраструктури, захист персональних даних і рівень довіри до державних інститутів. В умовах високої частки безготівкових операцій та значних масштабів соціальних виплат будь-яка масштабна кібератака, витік або порушення доступності сервісів трансформуються у ризик соціальної дестабілізації, зростання звернень громадян і виникнення спорів між сторонами, де ключового значення набувають докази, доказова база та процесуальні аспекти фіксації цифрових слідів у межах досудового розгляду справ і судового процесу.

Отже, інформаційна безпека фінансових установ повинна розглядатися як складова публічного інтересу та інфраструктурної стійкості держави, а її організаційно-правові засади мають будуватися на поєднанні ризик-орієнтованого регулювання, спроможної інституційної координації, стандартизованих процедур реагування й відновлення, контролю третіх сторін і забезпечення належної доказової бази для захисту прав отримувачів соціальної допомоги. Саме така інтегрована рамка підсилює здатність держави гарантувати безперервність фінансових сервісів у кризових умовах та підтримувати довіру громадян до цифровізованої системи соціальної підтримки.

Література:

1. Національний банк України. Безготівкові розрахунки у 2024 році суттєво переважали серед операцій з платіжними картками. 03.03.2025. URL: https:// bank.gov.ua/en/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami (дата звернення: 15.12.2025).
2. Міністерство фінансів України. У 2024 році в повному обсязі профінансовано соцвиплати на 447,9 млрд грн. 09.01.2025. URL: https:// kmu.gov.ua/en/news/minfin-u-2024-rotsi-v-povnomu-obsiazi-profinansovano-sotsvyplaty-na-4479-mlrd-hrn (дата звернення: 15.12.2025).
3. Державна служба спеціального зв'язку та захисту інформації України. CERT-UA минулого року опрацювала 4315 кіберінцидентів. 08.01.2025. URL: https:// cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 15.12.2025).
4. Національний банк України. Посилюється рівень інформаційної безпеки та кіберзахисту надавачів фінансових послуг. 12.12.2025. URL: https:// bank.gov.ua/ua/news/all/posilyuyetsya-riven-informatsiynoyi-bezpeki-ta-kiberzahistu-nadavachiv-finansovih-poslug (дата звернення: 15.12.2025).
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2015 № 2163-VIII. База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/2163-19 (дата звернення: 15.12.2025).
6. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 15.12.2025).
7. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/2297-17 (дата звернення: 15.12.2025).
8. Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. База даних Законодавство України / Верховна Рада України. URL: https:// zakon.rada.gov.ua/go/1591-20 (дата звернення: 15.12.2025).
9. EUR-Lex. Digital operational resilience for the financial sector. Summary. 10.01.2024. URL: https:// eur-lex.europa.eu/EN/legal-content/summary/digital-operational-resilience-for-the-financial-sector.html (дата звернення: 15.12.2025).
10. IBM. Cost of a data breach 2024: Financial industry. 2024. URL: https:// www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry (дата звернення: 15.12.2025).

References:

1. Natsionalnyi bank Ukrainy. (2025, March 3). Bezghotivkovi rozrakhunky u 2024 rotsi suttievo perevazhaly sered operatsii z platizhnymy kartkamy [Cashless payments in 2024 significantly prevailed among payment card transactions]. Natsionalnyi bank Ukrainy – National Bank of Ukraine. Retrieved from https:// bank.gov.ua/en/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami [in Ukrainian].

2. Ministerstvo finansiv Ukrainy. (2025, January 9). U 2024 rotsi v povnomu obsiazi profinansovano sotsvyplaty na 447,9 mlrd hrn [In 2024, social benefits were fully funded in the amount of UAH 447.9 billion]. Uriadovyi portal – Government Portal of Ukraine. Retrieved from https:// kmu.gov.ua/en/news/minfin-u-2024-rotsi-v-povnomu-obsiazi-profinansovano-sotsvyplaty-na-4479-mlrd-hrn [in Ukrainian].

3. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2025, January 8). CERT-UA mynuloho roku opratsiuvala 4315 kiberintsydentiv [CERT-UA processed 4,315 cyber incidents last year]. cip.gov.ua – Cybersecurity Information Portal. Retrieved from https:// cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv [in Ukrainian].

4. Natsionalnyi bank Ukrainy. (2025, December 12). Posyliuietsia riven informatsiinoi bezpeky ta kiberzakhystu nadavachiv finansovykh posluh [The level of information security and cyber protection of financial service providers is being strengthened]. Natsionalnyi bank Ukrainy – National Bank of Ukraine. Retrieved from https:// bank.gov.ua/ua/news/all/posilyuyetsya-riven-informatsiynoyi-bezpeki-ta-kiberzahistu-nadavachiv-finansovih-poslug [in Ukrainian].

5. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [Law of Ukraine On Basic Principles of Ensuring Cybersecurity of Ukraine]. (2017, October 5). zakon.rada.gov.ua. Retrieved from https:// zakon.rada.gov.ua/go/2163-19 [in Ukrainian].

6. Zakon Ukrainy Pro krytychnu infrastrukturu [Law of Ukraine On Critical Infrastructure]. (2021, November 16). zakon.rada.gov.ua. Retrieved from https:// zakon.rada.gov.ua/laws/show/1882-20 [in Ukrainian].

7. Zakon Ukrainy Pro zakhyst personalnykh danykh [Law of Ukraine On Personal Data Protection]. (2010, June 1). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/go/2297-17 [in Ukrainian].

8. Zakon Ukrainy Pro platizhni posluhy [Law of Ukraine On Payment Services]. (2021, June 30). zakon.rada.gov.ua. Retrieved from https:// zakon.rada.gov.ua/go/1591-20 [in Ukrainian].

9. EUR-Lex. (2024, January 10). Digital operational resilience for the financial sector. Summary. EUR-Lex. Retrieved from https:// eur-lex.europa.eu/EN/legal-content/summary/digital-operational-resilience-for-the-financial-sector.html [in English].

10. IBM. (2024). Cost of a data breach 2024: Financial industry. IBM. Retrieved from https:// www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry [in English].