Державне управління

УДК 35.073.526

Зайвелєв Юрій Ігорович

аспірант кафедри державного управління

Київського національного університету імені Тараса Шевченка

Zaiveliev Yurii

Postgraduate Student of the

Department of Public Administration

Taras Shevchenko National University of Kyiv

ORCID: 0009-0005-4382-096X

БЕЗПЕКА ЕЛЕКТРОННИХ ПЛАТЕЖІВ У СИСТЕМАХ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ В УМОВАХ КІБЕРЗАГРОЗ
SECURITY OF ELECTRONIC PAYMENTS IN PUBLIC ADMINISTRATION SYSTEMS IN THE FACE OF CYBER THREATS

Анотація. *Вступ. Електронні платежі стають все більш популярним способом спілкування між людьми, компаніями та державою. Цифрові фінансові операції зменшують адміністративні перешкоди, прискорюють надання державних послуг і роблять публічне адміністрування більш прозорим. Запровадження електронних платіжних систем для сплати податків, адміністративних зборів, штрафів та інших послуг стало важливим кроком у розвитку цифрової держави.*

Але ризики, пов'язані з кібератаками, фінансовим шахрайством, витоком конфіденційних даних і маніпуляцією транзакціями, зростають разом із розширенням доступу до державних електронних фінансових платформ. Ця проблема особливо важлива в умовах воєнного стану в Україні, оскільки державні платіжні системи можуть стати ціллю кібератак, які можуть дестабілізувати фінансовий сектор країни.

Таким чином, дослідження проблем, пов'язаних із безпекою електронних платежів у сфері публічного адміністрування, є важливою частиною захисту національної кіберінфраструктури, що вимагає розробки ефективних механізмів для боротьби з можливими небезпеками.

Мета. Метою статті є визначення головних ризиків, що виникли перед електронними платіжними системами у області публічного адміністрування, аналіз механізмів захисту від них та формулювання рекомендацій щодо підвищення безпеки цифрових розрахунків у державному секторі.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти, що регулюють електронні платежі та кібербезпеку в Україні; 2) міжнародні стандарти безпеки електронних платежів; 3) дослідження вітчизняних та зарубіжних авторів, що стосуються захисту фінансових даних у державному секторі.

Теоретичне узагальнення, формалізація, аналіз і логічне узагальнення результатів (формулювання висновків) були науковими методами, які використовувалися для проведення дослідження. Цей комплексний підхід було створено за допомогою цих методів; він включає системний і порівняльний аналіз, аналіз сучасних наукових джерел і моделювання організаційно-інформаційного забезпечення для ефективного цифрового управління. Крім того, було розглянуто конкретні випадки атак на платіжні платформи, які належать державі. Це дало можливість оцінити ефективність існуючих захисних заходів і визначити основні вразливості електронних фінансових послуг, які під контролем публічного адміністрування.

Результати. У дослідженні було виявлено, що електронні платежі в системах публічного адміністрування є важливою частиною цифрової держави, але вони все ще схильні до багатьох кіберзагроз. Аналіз показав, що основними небезпеками для державних платіжних систем є фішингові

атаки, витік персональних даних, несанкціонований доступ до фінансових ресурсів, атаки DDoS і маніпуляції з платіжними транзакціями. Крім того, було відзначено, що під час воєнного стану ймовірність кіберзлочинності значно зросла, що вимагає посилення заходів захисту.

Дослідження підтвердило, що впровадження міжнародних стандартів кібербезпеки, використання сучасних методів аутентифікації, використання блокчейн-технологій для гарантії незмінності даних і автоматизація аналізу фінансових операцій за допомогою штучного інтелекту визначають рівень кібербезпеки електронних платежів у державному секторі. Проведений аналіз вказує на те, що необхідно створити єдину стратегію захисту платіжних сервісів для держави. Ця стратегія має базуватися на багаторівневій моделі кібербезпеки та адаптивних механізмах реагування на кіберзагрози.

Перспективи. Подальші дослідження мають бути спрямовані на створення комплексної системи кіберзахисту державних електронних платежів. Застосування найновіших технологій криптографічного захисту, створення складних систем моніторингу загроз і розширення можливостей для міжнародної співпраці у сфері кібербезпеки є всіма прикладами цього. Особливу увагу слід привернути до вдосконалення законодавства щодо цифрових платежів і кіберзахисту, створення інфраструктури безпечних електронних платежів на національному рівні та розробки стандартів цифрової ідентифікації громадян.

Використання штучного інтелекту та аналітичних систем для виявлення аномалій у фінансових транзакціях може стати важливим компонентом боротьби з фінансовими злочинами. Крім того, важливим напрямком майбутніх досліджень є інтеграція технологій блокчейну в державні фінансові сервіси з метою підвищення рівня прозорості та захисту транзакцій від втручання ззовні. Створення

кіберінфраструктури, стійкої до атак, є стратегічно важливим завданням, яке потребує спільних зусиль науковців, урядових органів і міжнародних партнерів. Зважаючи на сучасні виклики, це завдання потребує спільних зусиль.

Ключові слова: *електронні платежі, публічне адміністрування, кібербезпека, цифрові фінансові послуги, державне управління, блокчейн, криптографічний захист, штучний інтелект, цифрова ідентифікація.*

Summary. *Introduction. Electronic payments are becoming an increasingly popular way of communicating between people, companies, and the state. Digital financial transactions reduce administrative barriers, speed up the delivery of public services, and make public administration more transparent. The introduction of electronic payment systems for paying taxes, administrative fees, fines, and other services has become an important step in the development of the digital state.*

However, the risks associated with cyberattacks, financial fraud, confidential data leakage, and manipulation of transactions are increasing as access to public electronic financial platforms grows. This problem is especially important in the context of martial law in Ukraine, as state payment systems may become a target of cyberattacks that could destabilize the country's financial sector.

Thus, the study of problems related to the security of electronic payments in the field of public administration is an important part of protecting the national cyber infrastructure, which requires the development of effective mechanisms to combat possible dangers.

Purpose. The purpose of the article is to identify the main risks faced by electronic payment systems in the field of public administration, to analyze the mechanisms of protection against them, and to formulate recommendations for improving the security of digital payments in the public sector.

Materials and methods. The research materials are: 1) legal acts regulating electronic payments and cybersecurity in Ukraine; 2) international standards for electronic payment security; 3) studies by domestic and foreign authors on the protection of financial data in the public sector.

Theoretical generalization, formalization, analysis, and logical summarization of the results (formulation of conclusions) were the scientific methods used to conduct the study. This comprehensive approach was created using these methods; it includes systematic and comparative analysis, analysis of modern scientific sources and modeling of organizational and information support for effective digital governance. In addition, specific cases of attacks on state-owned payment platforms were considered. This made it possible to assess the effectiveness of existing protective measures and identify the main vulnerabilities of electronic financial services under the control of public administration.

Results. The study found that electronic payments in public administration systems are an important part of the digital state, but they are still exposed to many cyber threats. The analysis showed that the main dangers to public payment systems are phishing attacks, personal data leakage, unauthorized access to financial resources, DDoS attacks, and manipulation of payment transactions. In addition, it was noted that during martial law, the likelihood of cybercrime has increased significantly, which requires strengthening of security measures.

The study confirmed that the implementation of international cybersecurity standards, the use of modern authentication methods, the use of blockchain technologies to guarantee data integrity, and the automation of financial transaction analysis using artificial intelligence determine the level of cybersecurity of electronic payments in the public sector. The analysis shows that it is necessary to create a unified strategy for protecting payment services

for the state. This strategy should be based on a multi-level cybersecurity model and adaptive mechanisms for responding to cyber threats.

Discussion. Further research should be aimed at creating a comprehensive cybersecurity system for public electronic payments. The use of the latest cryptographic protection technologies, the creation of sophisticated threat monitoring systems, and the expansion of opportunities for international cooperation in the field of cybersecurity are all examples of this. Particular attention should be paid to improving legislation on digital payments and cybersecurity, creating a secure electronic payment infrastructure at the national level, and developing standards for digital identification of citizens.

The use of artificial intelligence and analytical systems to detect anomalies in financial transactions can be an important component of the fight against financial crime. In addition, an important area for future research is the integration of blockchain technologies into public financial services to increase transparency and protect transactions from external interference. Creating a cyber infrastructure that is resistant to attacks is a strategically important task that requires joint efforts of scientists, government agencies, and international partners. Given the current challenges, this task requires joint efforts.

Key words: *electronic payments, public administration, cybersecurity, digital financial services, public administration, blockchain, cryptographic protection, artificial intelligence, digital identification.*

Постановка проблеми. Швидкий розвиток цифрових технологій і зростання обсягу електронних платежів є ознаками сучасних світових фінансово-економічних подій. У сфері публічного адміністрування впровадження електронних платіжних систем є важливим кроком до підвищення прозорості та ефективності державного управління. Уряди багатьох країн активно використовують цифрові платформи для безготівкового розрахунку, сплати податків, штрафів, адміністративних

зборів і соціальних виплат. Це допомагає оптимізувати державні фінанси, покращити доступ до державних послуг і зменшити бюрократію.

З іншого боку, зростання використання електронних платежів супроводжується збільшенням кількості кіберзагроз, які створюють серйозний ризик для державних фінансових систем. Кібератаки на платіжні системи можуть призвести до фінансових втрат, компрометації персональних даних громадян і дестабілізації роботи державних установ. Ця проблема є особливо важливою в умовах воєнного стану та гібридних загроз, коли державні фінансові системи є ціллю атак організованих кіберзлочинних груп і ворожих державних структур.

Фінансова інфраструктура стає більш вразливою через відсутність єдиних правил захисту державних електронних платежів, низьку обізнаність користувачів про потенційні ризики та обмеженість ресурсів для забезпечення кібербезпеки. Покращення безпеки цифрових платежів у сфері публічного адміністрування вимагає впровадження комплексних заходів. Ці заходи включають впровадження багаторівневої аутентифікації, покращення систем моніторингу транзакцій, посилення контролю за діяльністю фінансових посередників і впровадження сучасних технологій кіберзахисту. Таким чином, питання безпеки електронних платежів у публічному адмініструванні набуває стратегічного значення та потребує всебічного дослідження, щоб створити ефективні методи захисту та мінімізації ризиків фінансових та інформаційних злочинів.

Аналіз останніх досліджень і публікацій. Науковці в Україні та за кордоном активно досліджують проблеми безпеки електронних платежів у публічному адмініструванні. Вони зосереджуються на цифровій безпеці, контролі електронних фінансових транзакцій, впровадженні сучасних технологій захисту та оцінці впливу кіберзагроз на державні платіжні системи.

У статті Євгена Живило «Актуальні проблеми кібербезпеки в системах електронних комунікацій учасників фінансового ринку України з урахуванням міжнародних практик у цій галузі» аналізується сучасний стан кібербезпеки фінансових комунікацій в Україні та підкреслюється необхідність впровадження національних стандартів кібербезпеки, щоб захистити електронні платежі [1].

У своїй монографії «Фінансові технології» Олена Іванівна Береславська та Андрій Іванович Гулей досліджують вплив фінансових технологій на модернізацію економіки та фінансової системи України. Автори підкреслюють важливість цифрової безпеки в умовах зростаючої цифровізації [2].

У статті «Управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення» Л.В. Мазник та З.П. Двуліт розглядають питання управління кібербезпекою в умовах військових конфліктів, підкреслюючи важливість підготовки кваліфікованих працівників для захисту державних платіжних систем [3].

Дослідники також звертають увагу на безпеку електронних платежів на міжнародному рівні. Організація економічного співробітництва та розвитку (OECD) аналізує методи підвищення стійкості цифрових фінансових систем України та пропонує сучасні технології захисту [4].

Таким чином, аналіз досліджень свідчить про те, що для забезпечення кібербезпеки електронних платежів у публічному адмініструванні необхідно використовувати комплексний підхід, який включає розробку національних стандартів, впровадження сучасних технологій захисту та навчання кваліфікованих фахівців у сфері кібербезпеки.

Формулювання цілей статті. Мета статті полягає в тому, щоб визначити основні загрози безпеці електронних платежів у системах публічного адміністрування, проаналізувати сучасні методи захисту цих

платежів і розробити поради щодо підвищення кібербезпеки державних фінансових платформ, особливо під час воєнного стану.

Виклад основного матеріалу. Щоб зробити державні послуги більш ефективними, зробити фінансові операції більш ефективними та зробити адміністративні процеси більш прозорими, сучасний етап розвитку державного управління характеризується активною цифровою трансформацією. Впровадження електронних платежів у систему публічного адміністрування було важливим кроком у цьому напрямку, оскільки це дозволяє громадянам і компаніям проводити фінансові операції швидше, зручніше та безпечніше.

Цифровізація фінансових операцій у державному секторі призводить до нових проблем, особливо у сфері кібербезпеки, незважаючи на численні переваги. У зв'язку з зростаючими ризиками шахрайства, кібератак, витоку персональних даних і ймовірністю зловживання адміністративними ресурсами необхідно використовувати сучасні технології захисту. Це особливо важливо зараз, коли в Україні триває війна, оскільки російська агресія поставила під загрозу фінансову стабільність країни, включаючи цілеспрямовані атаки на державні платіжні системи, банківські установи та електронні сервіси.

В умовах війни державні електронні фінансові платформи стали не лише засобом оплати, а й важливою частиною соціального забезпечення. Громадяни можуть дистанційно отримувати виплати, допомогу для внутрішньо переміщених осіб, компенсації та субсидії завдяки цифровим технологіям, які є життєво важливими у період гуманітарної кризи. Однак противник активно використовує кіберзброю, щоб дестабілізувати цю систему. У зв'язку з масовими DDoS-атаками, спробами перехоплення транзакцій і маніпуляціями з фінансовими даними уряди повинні вдосконалювати свої системи захисту та дотримуватися міжнародних стандартів кібербезпеки.

Кіберзлочинці неодноразово атакували українську фінансову систему в останні роки, здійснюючи масштабні атаки на банківські сервіси та державні платіжні платформи. Одним із найгучніших випадків була DDoS-атака на Монобанк у 2022 році, яка зупинила онлайн-банкінг і заблокувала платежі. Перевантаження серверів спричинило значні незручності як для бізнесу, так і для громадян, оскільки користувачі не могли отримати доступ до своїх рахунків, оплачувати чи пересилати гроші. Інші комерційні банки, такі як ПриватБанк і ОщадБанк, також були об'єктами подібних атак. Вони поставили під загрозу онлайн-банкінг і системи прийому платежів через термінали.

Кіберзлочинці використовують фішингові схеми, щоб отримати доступ до персональних даних громадян, крім DDoS-атак. Одним із прикладів є масштабна фішингова кампанія, спрямована на користувачів системи «Дія», у якій шахраї створювали підроблені сайти для крадіжки банківських реквізитів. Вони використовували соціальну інженерію, щоб переконати людей вводити свої дані, щоб вони нібито отримали гроші, але насправді вони втратили гроші.

Контроль над транзакціями в державних платіжних системах є ще одним типом атак, який став більш поширеним. Наприклад, у 2023 році було виявлено випадки підміни реквізитів під час перерахування соціальних виплат; це дозволило зловмисникам переадресовувати гроші на шахрайські рахунки.

Захист персональних даних громадян залишається значним викликом. Злом електронних реєстрів може бути дуже шкідливим, зокрема для безпеки військових або осіб, які перебувають на тимчасово окупованих територіях. Зміцнення стійкості державних платіжних платформ залежить від впровадження багаторівневої аутентифікації, використання криптографічних методів шифрування та використання штучного інтелекту для відстеження транзакцій.

В Україні було вжито низку заходів, щоб зменшити ймовірність атак і підвищити безпеку державних електронних платежів. Більшість державних і фінансових платформ почали вимагати двофакторну автентифікацію (2FA) для підтвердження особи користувача, що значно ускладнило несанкціонований доступ до фінансових даних. Крім того, високотехнологічні криптографічні алгоритми активно застосовуються для шифрування даних під час їх передачі між користувачем і сервером.

Для підвищення рівня кібербезпеки у сфері публічного адміністрування необхідно продовжувати впроваджувати новітні технології та вдосконалювати регуляторну базу. Щоб гарантувати незмінність і прозорість державних платежів, децентралізовані реєстри, засновані на блокчейні, унеможливлять маніпуляції з транзакціями.

Крім того, вкрай важливо активно створювати автоматизовані системи реагування на загрози. Ці системи можуть аналізувати підозрілі фінансові операції в режимі реального часу та негайно блокувати потенційно шахрайські транзакції. Запровадження додаткових перевірок для небанківських установ допоможе зменшити ймовірність шахрайства.

Зміцнення міжнародної співпраці у сфері кібербезпеки також є важливим напрямом, оскільки це дозволить обмінюватися досвідом і інтегрувати найкращі світові практики захисту даних. Удосконалення законодавства для відповідності міжнародним стандартам безпеки, таким як PSD2 та GDPR, покращить захист даних громадян.

Таким чином, необхідно продовжувати розвивати системи кібербезпеки, використовувати нові технології та посилювати регулювання, щоб ефективно захистити державні фінансові сервіси від потенційних небезпек. У сфері публічного адміністрування лише комплексний підхід може гарантувати безпеку та стабільність цифрових платежів і мінімізувати ризики кіберзлочинності.

Очевидно, що обмежене фінансування є основним викликом для впровадження онлайн-платіжних систем у публічному адмініструванні. Це робить розробку та інтеграцію сучасних технологічних рішень складною. Економічні проблеми, спричинені війною, змушують державу спрямовувати ресурси на оборонні та соціальні потреби, не підтримуючи цифрові ініціативи. Водночас важливим залишається питання залучення альтернативних джерел фінансування, таких як гранти фінансових організацій, державно-приватне партнерство та технічна допомога за кордоном, яка дозволила б продовжувати розвиток цифрових фінансових послуг у державному секторі.

Окрім проблем з грошима, є багато технічних перешкод. Упровадження електронних платежів у державному управлінні значно ускладнюється браком інфраструктури, застарілими інформаційними системами та обмеженим доступом до Інтернету, особливо в сільських та прифронтових районах. Згідно з дослідженнями, оновлення цифрової інфраструктури є життєво важливим для забезпечення доступності Інтернет-платіжних послуг у всіх регіонах країни.

Не менш серйозним викликом є перешкоди, пов'язані з організацією та управлінням. Розбалансованість процесу цифровізації виникає через відсутність єдиної стратегії розвитку цифрових платежів у державному секторі та фрагментарність законодавчої бази. Наявні правила, що регулюють електронні фінансові операції, часто не відповідають сучасним стандартам і не враховують міжнародні стандарти кібербезпеки. Зокрема, необхідно посилити законодавство щодо захисту персональних даних і боротьби з кіберзлочинністю, щоб зробити державні веб-сайти безпечними.

Недостатня цифрова грамотність громадян і державних службовців є ще одним значним фактором, що перешкоджає розвитку електронних платежів у публічному адмініструванні. Багато людей продовжують

віддавати перевагу звичайним фінансовим операціям через недовіру до цифрових сервісів або погане розуміння того, як вони працюють. Крім того, державні установи стикаються з проблемою нестачі кваліфікованих працівників у сфері IT та кібербезпеки. Це робить розробку та впровадження ефективних цифрових рішень більш складним завданням. Згідно з дослідженнями, однією з основних причин неефективності цифрових реформ є дефіцит спеціалістів у сфері публічного адміністрування.

Отже, для подолання цих проблем потрібен комплексний підхід, який включає фінансову підтримку цифрових ініціатив, модернізацію технологічної інфраструктури, удосконалення нормативно-правової бази та підвищення рівня цифрової грамотності населення та працівників державного сектору. Завдяки синхронному вирішенню цих проблем можна досягти високого рівня ефективності та безпеки державних онлайн-платіжних систем, що сприятиме розвитку цифрового публічного адміністрування.

Висновки і перспективи подальших досліджень. Таким чином, впровадження електронних платіжних систем у сфері публічного адміністрування є важливим етапом цифрової трансформації державного управління. Ці системи покращують якість фінансових послуг, зменшують бюрократію та роблять фінансові операції більш прозорими. Однак недостатнє фінансування, технічні обмеження, регуляторні прогалини та низький рівень цифрової грамотності населення – це деякі з проблем, які перешкоджають цифровізації. Усунення цих перешкод є необхідною умовою створення надійної, безпечної та ефективної системи електронних платежів для державних цілей. Коли вони знають про проблеми кібербезпеки, потенційні загрози шахрайства та недоліки фінансової інфраструктури, держави можуть змінити свої існуючі засоби захисту та

створювати кращі моделі управління електронними фінансовими потоками.

Дослідження повинні зосередитися на вдосконаленні законодавства щодо цифрових фінансових операцій, кібербезпеці електронних платежів і підвищенні обізнаності громадян щодо безпечного використання державних онлайн-сервісів. Крім того, вивчення міжнародного досвіду цифрових фінансових технологій і можливостей їх адаптації до українських реалій є важливим напрямом. Розробка комплексного підходу до оцінки ефективності впровадження електронних платіжних систем дозволить не лише покращити їхню роботу, але й визначити найкращі шляхи подальшої цифровізації державного управління.

Література

1. Живило Є. О. Актуальні проблеми кібербезпеки в системах електронних комунікацій учасників фінансового ринку України з урахуванням міжнародних практик у цій сфері. *Публічне управління XXI століття: особливості воєнного і післявоєнного періодів: XXIII Міжнародний науковий конгрес.* Харків, 2023. С. 485–488. URL: https://www.researchgate.net/publication/380908571_Aktualni_problemi_kiberbezpeki_v_sistemah_elektronnih_komunikacij_ucasnikiv_finansovogo_rinku_Ukraini_z_urahuvannam_miznarodnih_praktik_u_cij_sferi (дата звернення: 13.02.2025).

2. Береславська О. І., Гулей А. І. Фінансові технології: навчальний посібник. Дніпро: Дніпровський національний університет імені Олеся Гончара, 2022. 260 с. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-metodicna%20literatura/F/Finansovi%20tehnologii.pdf (дата звернення: 13.02.2025).

3. Мазник Л. В., Двуліт З. П. Управління діяльністю фахівців з

кібербезпеки в умовах повномасштабного вторгнення. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку.* 2023. № 2 (9). С. 54–65. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2023/dec/32677/menedzhment223maket-54-65.pdf (дата звернення: 13.02.2025).

4. Організація економічного співробітництва та розвитку (OECD). Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. 2024. URL: https://www.oecd.org/content/dam/oecd/uk/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/5d9e86a7-uk.pdf (дата звернення: 14.02.2025).

References

1. Actual problems of cybersecurity in electronic communication systems of financial market participants in Ukraine, taking into account international practices in this area. *Public Administration of the XXI Century: Peculiarities of the Military and Postwar Periods: XXIII International Scientific Congress*. Kharkiv, 2023. C. 485-488. URL: https://www.researchgate.net/publication/380908571_Aktualni_problemi_kiberbezpeki_v_sistemah_elektronnih_komunikacij_ucasnikiv_finansovogo_rinku_Ukraini_z_urahuvannam_miznarodnih_praktik_u_cij_sferi [in Ukrainian].

2. Bereslavska O.I., Hulei A.I. Financial technologies: a textbook. Dnipro: Oles Honchar Dnipro National University, 2022. 260 c. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-metodicna%20literatura/F/Finansovi%20tehnologii.pdf [in Ukrainian].

3. Maznyk L. V., Dvulit Z. P. Management of cybersecurity specialists in the conditions of a full-scale invasion. *Management and entrepreneurship in Ukraine: stages of formation and development problems*. 2023. № 2 (9). C. 54-65. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2023/dec/32677/menedzhment223maket-54-65.pdf [in Ukrainian].

4. Organization for Economic Cooperation and Development (OECD). Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. 2024. URL: https://www.oecd.org/content/dam/oecd/uk/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/5d9e86a7-uk.pdf [in Ukrainian].