ДЕРЖАВНЕ АГЕНТСТВО ВІДНОВЛЕННЯ ТА РОЗВИТКУ ІНФРАСТРУКТУРИ УКРАЇНИ

НАУКОВА СПІЛЬНОТА «АСПІРАНТИ І ДОКТОРАНТИ УКРАЇНИ»

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ФІЗИЧНОГО ВИХОВАННЯ І СПОРТУ УКРАЇНИ
КАФЕДРА ТУРИЗМУ

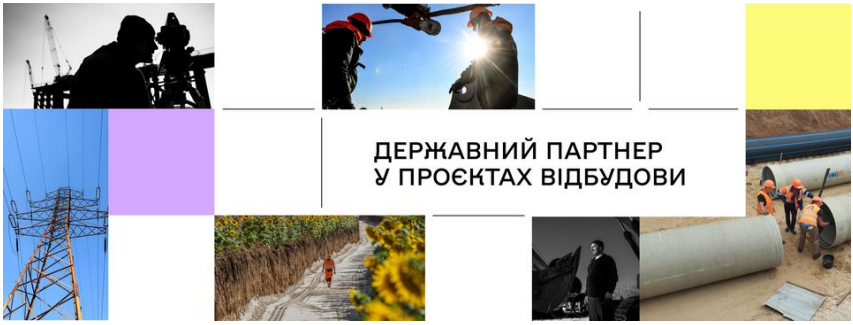
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОНСТИТУЦІЙНОГО ТА АДМІНІСТРАТИВНОГО ПРАВА

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
«ЦИФРОВІ ТЕХНОЛОГІЇ У ВІДНОВЛЕННІ ЕКОНОМІКИ ТА ІНФРАСТРУКТУРИ УКРАЇНИ»

CONFERENCE PROCEEDINGS

I INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE
"DIGITAL TECHNOLOGIES IN RECOVERY OF ECONOMY AND INFRASTRUCTURE OF UKRAINE"



2024

Шановні учасники та гості
І Міжнародної науково-практичної конференції
«Цифрові технології у відновленні економіки та інфраструктури України»

Від імені Державного агентства відновлення та розвитку інфраструктури України радий вітати Вас в рамках проведення І Міжнародної науково-практичної конференції ***«Цифрові технології у відновленні економіки та інфраструктури України»***.

У надзвичайно важкий для нашої країни час питання електронного урядування, цифровізації суспільних та державних послуг, інфраструктурного розвитку та відновлення є вкрай важливими і потребують посиленої уваги, особливо зі сторони наукової та освітянської спільноти. Ми вдячні кожному з Вас за Ваш внесок у пріоритетні напрями досліджень, які були розглянуті на конференції і впевнені, що ваші напрацювання матимуть своє практичне втілення на благо розвитку нашої країни.

Щиро переконаний, що проведення таких науково-практичних заходів сприятиме посиленню співпраці між нашим Агентством та науковою спільнотою і стане драйвером змін.

З найкращими побажаннями,
Роман Комендант, *заступник Голови Державного агентства відновлення та розвитку інфраструктури України з питань цифрового розвитку, цифрових трансформацій і цифровізації*

Науковий/програмний комітет:

КОМЕНДАНТ Роман – *в. о. Голови Державного агентства відновлення та розвитку інфраструктури України.*

ГУДИМА Ірина – *начальник Управління цифрового та інноваційного розвитку Державного агентства відновлення та розвитку інфраструктури України.*

БЕЗУГЛИЙ Артем - *кандидат економічних наук, доцент, директор Державного підприємства «Національний інститут розвитку інфраструктури», дійсний член Транспортної академії України, Почесний дорожник.*

БОНДАР Олена – *доктор економічних наук, кандидат технічних наук, професор, начальник Центру інноваційно-наукового розвитку та співробітництва Державного підприємства «Національний інститут розвитку інфраструктури».*

ШАТІЛО Володимир - *доктор юридичних наук, професор, Заслужений юрист України, завідувач кафедри конституційного та адміністративного права Національного транспортного університету***.**

ЗАХАРІН Сергій – *доктор економічних наук, старший науковий співробітник, заступник Голови Державної служби України з питань безпечності харчових продуктів та захисту споживачів з питань цифрового розвитку, цифрових трансформацій і цифровізації***.**

БАБУШКО Світлана – *доктор педагогічних наук, професор, завідувач кафедри туризму Національного університету фізичного виховання і спорту України***.**

СМЕНТИНА Наталія *- доктор економічних наук, професор, професор кафедри "Економіка і фінанси" Одеського національного морського університет.*

ЛАРІНА Ярослава *– доктор економічних наук, професор, професор кафедри маркетингу імені А. Ф. Павленка Київського національного економічного університету імені Вадима Гетьмана.*

KAPRANOV Yan *- Doctor of Sciences (Philology), Professor, Assistant Professor of the University of Economics and Human Sciences in Warsaw (Poland), the University of Oulu (Finland).*

IWANOWSKA Bożena *- Doctor of Social Sciences, Assistant Professor of the University of Economics and Human Sciences in Warsaw (Poland).*

ХУСАІНОВ Руслан *– завідувач сектору захисту інформаційних систем Управління цифрового та інноваційного розвитку Державного агентства відновлення та розвитку інфраструктури України.*

Видання здійснено за організаційної, технічної та інформаційної підтримки **Державного агентства відновлення та розвитку інфраструктури України**.

https://restoration.gov.ua/

Збірник матеріалів містить наукові роботи учасників І Міжнародної науково-практичної конференції **«ЦИФРОВІ ТЕХНОЛОГІЇ У ВІДНОВЛЕННІ ЕКОНОМІКИ ТА ІНФРАСТРУКТУРИ УКРАЇНИ»**, яка була проведена **13 листопада 2024 року**.

Збірник матеріалів конференції розміщено для вільного використання:

Роботи учасників конференції індексуються у Google Scholar:

Наукові роботи учасників конференції присвячені актуальним питанням досліджень у сфері державного управління, цифровізації, кібербезпеки, публічного адміністрування, міжнародних відносин, політології, туризму, економіки, інформаційних технологій, практичним аспектам повоєнного відновлення України, підприємництва та іншим важливим аспектам гуманітарного та соціально-економічного розвитку в сучасних умовах.

Збірник буде корисний науковцям, докторантам, аспірантам, працівникам системи освіти, державним службовцям, студентам.

Автори опублікованих матеріалів висловлюють свою думку, яка не завжди збігається з позицією редакції. За достовірність інформації, розміщеної у наукових роботах, відповідальність несуть автори даних робіт.

Мови публікації: українська, англійська.

Цитувати як:

ЦИФРОВІ ТЕХНОЛОГІЇ У ВІДНОВЛЕННІ ЕКОНОМІКИ ТА ІНФРАСТРУКТУРИ УКРАЇНИ: матеріали І Міжнар. наук.-практ. конф., 13 листопада 2024 р. – Київ : Державне агентство відновлення та розвитку інфраструктури України, 2024 р.

ДОРОГИЙ Ярослав,
д.т.н., проф., професор кафедри прикладної математики,
Донецький національний технічний Університет
cisco.rna@gmail.com
ЦУРКАН Василь,
к.т.н., доц., доцент спеціальної кафедри №5,
Інститут спеціального зв'язку та захисту інформації
КПІ ім. Ігоря Сікорського
v.v.tsurkan@gmail.com
БЕРДИЧЕНКО Ірина,
к.ю.н., старший викладач кафедри
цивільного та кримінального права і процесу,
Чорноморський національний університет імені Петра
Могили,
irinaberdychenko@gmail.com

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ БАНКІВСЬКОЇ СФЕРИ УКРАЇНИ

Анотація. Стаття розглядає питання кібербезпеки критичної інфраструктури банківської сфери України, яка є важливим елементом фінансової та національної безпеки держави. Особлива увага приділяється основним загрозам, що виникають перед банківськими установами, ролі секторальних органів у забезпеченні безпеки, а також шляхам вдосконалення існуючих механізмів захисту. Розглянуто додаткові виклики для банківського сектору, пов'язані з військовою агресією рф, а також представлені

рекомендації для підвищення кіберстійкості банківської сфери України.

Вступ. Банківська сфера України є однією з ключових складових економіки, що забезпечує стабільність фінансової системи та доступ населення до фінансових послуг. В умовах цифровізації банківської діяльності, посилення кіберзагроз, а також військової агресії з боку рф, захист критичної інфраструктури банківської сфери набуває особливого значення. *Метою дослідження* є аналіз сучасного стану кібербезпеки в банківському секторі України з урахуванням нових викликів, пов'язаних із зовнішньою агресією, а також розробка рекомендацій щодо вдосконалення системи захисту критичної банківської інфраструктури.

Захист критичної інфраструктури банківської сфери. Захист критичної інфраструктури банківської сфери є важливою умовою забезпечення фінансової стабільності та національної безпеки України. Критична інфраструктура банків включає систему обробки платежів, канали передачі фінансових даних, бази даних клієнтів, а також системи онлайн-банкінгу. Відмова або порушення роботи цих елементів можуть мати серйозні економічні наслідки та призвести до зниження довіри до банківської системи.

Військова агресія російської федерації створює додаткові ризики для банківської сфери України. Серед них виділяються

кібератаки з боку державних та підтримуваних рф хакерських угруповань, спрямовані на дестабілізацію фінансової системи. Такі атаки можуть бути масштабними та мати на меті порушення роботи банківських систем, виведення з ладу платіжних інфраструктур та компрометацію даних клієнтів. Напади на критичну інфраструктуру під час війни створюють значний тиск на банки та вимагають підвищення рівня захисту.

Основу регулювання кібербезпеки банківської сфери в Україні складає Закон України «Про основні засади забезпечення кібербезпеки України» [1], який встановлює базові вимоги та принципи захисту інформаційних систем об’єктів критичної інфраструктури. Згідно зі статтею 19 Закону України "Про критичну інфраструктуру", основні завдання Національного банку України (НБУ) полягають у забезпеченні безпеки об'єктів банківської критичної інфраструктури, включаючи визначення та оцінку критичних банківських установ, розробку нормативно-правових актів, що регулюють їх захист, а також координацію заходів із захисту цієї інфраструктури в разі надзвичайних ситуацій. НБУ відповідає за організацію моніторингу, аудиту та оцінки стану кібербезпеки банків, встановлює вимоги до системи управління безпекою та проводить заходи щодо вдосконалення механізмів захисту банківських установ від кіберзагроз [2].

Також, до законів, які відіграють важливе значення для регулювання процесів захисту критичної інфраструктури банківської сфери відноситься Закон України «Про Національний банк України» [3]. Саме цим Законом визначено, що Національний банк України забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури щодо банків, інших осіб, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг відповідно до закону, що визначає правові та організаційні засади функціонування і захисту критичної інфраструктури, та передбачено низку повноважень Національного банку України із захисту критичної інфраструктури банківської сфери.

В умовах війни міжнародне співробітництво також є важливим елементом захисту банківської інфраструктури. Співпраця з Європейським агентством з кібербезпеки (ENISA) та запровадження міжнародних стандартів інформаційної безпеки, зокрема ISO/IEC 27001 [4], допомагають українським банкам використовувати передові технології та методики для виявлення загроз. Українські банки також отримують підтримку від

міжнародних партнерів у вигляді консультацій, доступу до бази знань про новітні кібератаки та їх індикатори.

Незважаючи на зусилля банківського сектору та державних органів, виклики, пов'язані з війною, значно ускладнюють забезпечення кібербезпеки. Військові дії посилюють загрози інсайдерських атак, коли неналежна поведінка співробітників може призвести до витоку інформації. Крім того, кібератаки стають дедалі витонченішими та часто випереджають темпи впровадження захисних технологій. Відсутність доступу до критичних ресурсів через активні бойові дії та обмеженість кваліфікованих кадрів також негативно впливають на рівень безпеки банків.

З метою підвищення захисту критичної інфраструктури банківської сфери слід зазначити кілька ключових завдань, які було б доцільно розв'язати на рівні профільного управління НБУ:

1. Координація між підрозділами

– *інтеграція зусиль* – управління може виконувати роль моста між різними департаментами, які займаються фізичною безпекою, кібербезпекою та іншими аспектами. Це дозволить створити єдину стратегічну платформу для захисту критичної інфраструктури, уникнувши дублювання зусиль і забезпечивши консистентність у застосуванні заходів.

– *спільні ініціативи* – розробка спільних проектів та програм, які об'єднують різні напрямки безпеки, може допомогти у

формуванні комплексного підходу до захисту. Наприклад, інтеграція кібербезпеки з фізичною безпекою у програмах навчання або у внутрішніх політиках банків.

2. Аналіз і управління ризиками

– *централізований аналіз ризиків* – управління може зосередитися на проведенні всебічного аналізу ризиків для всіх аспектів критичної інфраструктури, що дозволить ідентифікувати системні вразливості, які можуть бути неочевидними для окремих департаментів.

– *крос-функціональні групи* – формування та координація крос-функціональних команд, які складаються з представників різних департаментів для оцінки ризиків і розробки стратегії їх управління, може покращити загальну ситуацію з безпекою.

3. Стандартизація та регуляція

– *розробка стандартів* – хоча інші підрозділи можуть реалізовувати окремі заходи, Управління може сфокусуватися на координації створення єдиних стандартів для всіх аспектів захисту критичної інфраструктури. Це забезпечить єдине розуміння безпеки в усіх банках і дасть змогу спростити перевірки та аудит.

– *системи контролю* – впровадження єдиних систем контролю для моніторингу відповідності стандартам/настановам у

сфері захисту критичної інфраструктури у всіх банківських установах.

4. Освіта та навчання

– *розробка навчальних програм* – управління може займатися розробкою навчальних програм, які охоплюють всі аспекти захисту критичної інфраструктури банківської сфери, зосереджуючи увагу на міждисциплінарному підході. Це навчання має бути обов'язковим для співробітників усіх рівнів.

– *семінари та тренінги* – організація регулярних семінарів та тренінгів, які сприяють обміну досвідом та кращими практиками між різними підрозділами та установами.

5. Стратегічне партнерство та співпраця

– *співпраця з міжнародними організаціями* – управління може розвивати партнерства з міжнародними організаціями та іншими регуляторами для обміну інформацією та досвідом у сфері захисту критичної інфраструктури.

– *участь у галузевих ініціативах* – участь у створенні міжнародних стандартів безпеки критичної інфраструктури банківської сфери, що дозволяє Україні бути на одному рівні з іншими країнами.

6. Моніторинг та оцінка ефективності

– *створення системи моніторингу* – управління може розробити систему моніторингу та оцінки ефективності всіх

заходів, що впроваджуються, з метою ефективної реакції на нові виклики та коригування стратегій, настанов тощо.

– *регулярні звіти* – управління повинно забезпечити формування консолідованих звітів про стан критичної інфраструктури для всіх учасників процесу, що дозволить зберігати прозорість і відповідальність.

7. Інновації та технології

– *впровадження нових технологій* – управління може сфокусуватися на дослідженні доцільності впровадження інноваційних технологій у сфері безпеки, розробці методик їх впровадження в таких сферах, як автоматизовані системи моніторингу, аналітика великих даних та штучний інтелект, що можуть підвищити ефективність захисту критичної інфраструктури.

– *розробка пілотних проектів* – ініціювання пілотних проектів для тестування нових технологій у реальних умовах.

8. Кризове управління

– *планування кризових сценаріїв* – розробка сценаріїв реагування на можливі кризові ситуації, пов'язані з загрозами для критичної інфраструктури, та підготовка планів дій.

– *навчання з кризового управління* – проведення навчань для персоналу банків з метою підвищення їхньої готовності до реагування на надзвичайні ситуації.

9. Підтримка відновлення

– *план відновлення* – розробка стратегії відновлення критичної інфраструктури після надзвичайних ситуацій, що включає в себе адаптацію до нових умов та покращення існуючих систем.

– *фінансування відновлення* – визначення механізмів фінансування для швидкого відновлення критичної інфраструктури після кризових ситуацій.

10. Публічна комунікація

– *інформаційні кампанії* – організація інформаційних кампаній для підвищення обізнаності про важливість захисту критичної інфраструктури серед населення та підприємств.

– *зворотний зв'язок* – встановлення механізмів для збору відгуків від банків і споживачів щодо заходів безпеки, що впроваджуються, для їх покращення.

11. Розробка нормативно-правових актів з унормування питань захисту критичної інфраструктури банківської сфери щодо:

– ідентифікації та категоризації банківської інфраструктури, як об’єктів критичної інфраструктури;

– особливостей паспортизації об’єктів критичної інфраструктури;

– розроблення вимог до захисту об’єктів критичної інфраструктури;

– визначенням проєктних та об’єктових загроз критичній інфраструктурі.

Висновки. З початком військової агресії рф проти України збільшились ризики для критичної інфраструктури банківської сфери, що потребує від банків та держави швидкої адаптації до нових загроз. Для забезпечення безпеки банківської інфраструктури необхідно реалізувати комплексні заходи, включаючи удосконалення нормативно-правової бази, інтеграцію сучасних технологій моніторингу та кіберзахисту, а також створення ефективних резервних систем для підтримки операційної діяльності в кризових ситуаціях. Паралельно важливо зміцнювати міжнародне співробітництво, обмінюючись досвідом із партнерами та запроваджуючи кращі практики для зниження впливу зовнішніх загроз. Тільки за умови синергії регуляторних, технологічних і організаційних заходів можна забезпечити стабільність фінансової системи та зберегти її цілісність у цей складний період.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України, 5 жовтня 2017 року, № 2163-VIII / Верховна Рада України (онлайн) URL:

https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02 листопада 2024).

2. Про критичну інфраструктуру: Закон України, 16 листопада 2021 року, № 1882-IX / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 02 листопада 2024).

3. Про Національний банк України: Закон України від 20 травня 1999 року № 679-XIV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/679-14 (дата звернення: 02 листопада 2024).

4. ISO/IEC 27001:2013 Information security management systems — Requirements / International Organization for Standardization. URL: https://www.iso.org/standard/27001 (дата звернення: 02 листопада 2024).

ЗМІСТ

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
«ЦИФРОВІ ТЕХНОЛОГІЇ У ВІДНОВЛЕННІ ЕКОНОМІКИ ТА ІНФРАСТРУКТУРИ УКРАЇНИ»

CONFERENCE PROCEEDINGS

I INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE
"DIGITAL TECHNOLOGIES IN RECOVERY OF ECONOMY AND INFRASTRUCTURE OF UKRAINE"

Відповідальний за випуск – Солодов О.П.

Дизайн і верстка – Головняк І.В.

Київ - 2024