МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
БІЛОЦЕРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ

ОПП «Публічне управління та адміністрування»

Допускається до захисту
Завідувач кафедри публічного управління,
адміністрування та міжнародної економіки
назва кафедри
професор Сокольська Т.В.
підпис, вчене звання, прізвище, ініціали
« 25 » листопада 2025 року

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

(за матеріалами Державної служби України з безпеки на транспорті)

Виконав: Швець В'ячеслав Віталійович
прізвище, ім'я, по батькові, підпис
Керівник: доцент Панасюк Вікторія Іллівна
вчене звання, прізвище, ім'я, по батькові підпис
Рецензент: доцент Гаврик Олеся Юріївна
вчене звання, прізвище, ім'я, по батькові підпис

Я, Швець В'ячеслав Віталійович, засвідчую, що кваліфікаційну роботу магістра виконано з дотриманням принципів академічної доброчесності.

Біла Церква – 2025

РЕФЕРАТ

Швець В'ячеслав Віталійович Удосконалення механізмів забезпечення інформаційної безпеки в системі публічного управління в умовах цифрової трансформації (за матеріалами Державної служби України з безпеки на транспорті)

Досліджено особливості процесу забезпечення інформаційної безпеки в умовах цифрової трансформації в органах публічного управління України та в Державній службі безпеки на транспорті зокрема.

Використано структурно-функціональний аналіз – для дослідження організаційної моделі забезпечення ІБ у ДСБТ; ризик-орієнтований аналіз – для ідентифікації загроз, вразливостей та визначення рівня ризиків інформаційної безпеки в ДСБТ.

Виявлено сутність інформаційної безпеки в системі публічного управління, охарактеризовано вплив цифрової трансформації на формування сучасної моделі ІБ державного сектору, досліджено нормативно-правові, організаційні та управлінські механізми забезпечення інформаційної безпеки в Державній службі України з безпеки на транспорті, досліджено існуючі інструменти кіберзахисту, оцінено ефективність чинних механізмів забезпечення інформаційної безпеки ДСБТ, виявлено ключові ризики, загрози та вразливості інформаційній безпеці ДСБТ в умовах цифрової трансформації, обґрунтувано комплекс практичних рекомендацій щодо впровадження сучасних засобів кіберзахисту, оптимізації управління інцидентами, підвищення цифрової компетентності персоналу та розвитку культури кібергігієни, проведено економічне оцінювання ефективності запропонованих заходів, визначено інтегральний економічний ефект від їх реалізації та обґрунтовано доцільність впровадження.

Зроблено висновок, що Державна служба України з безпеки на транспорті відіграє ключову роль у забезпеченні захищеності інформаційних потоків у сфері транспортної безпеки, а рівень кіберзахисту її систем безпосередньо впливає на стабільність роботи інфраструктури та довіру громадян до державних сервісів. Практична значущість результатів дослідження полягає у створенні практичних рекомендацій щодо вдосконалення механізмів забезпечення інформаційної безпеки в системі публічного управління в умовах цифрової трансформації.

Кваліфікаційна робота магістра містить 88 сторінок, 15 таблиць, 10 рисунків, список використаних джерел із 45 найменувань.

Ключові слова: інформаційна безпека, кіберзахист, цифрова трансформація, публічне управління, кіберзагрози, управління інцидентами, цифрова компетентність.

ANNOTATION

Shvets Viacheslav Vitaliiovych Improvement of Mechanisms for Ensuring Information Security in the Public Administration System under the Conditions of Digital Transformation (based on materials from the State Service of Ukraine for Transport Safety)

The features of the information security process under conditions of digital transformation in the public administration bodies of Ukraine, and in the State Service for Transport Safety in particular, have been examined

A structural and functional analysis was applied to examine the organizational model of information security in the State Service for Transport Safety; a risk-oriented analysis was used to identify threats, vulnerabilities, and to determine the level of information security risks within the agency.

The essence of information security in the public administration system has been revealed; the impact of digital transformation on the formation of a modern information security model in the public sector has been characterized; the regulatory, organizational, and managerial mechanisms of information security within the State Service of Ukraine for Transport Safety have been examined; existing cybersecurity tools have been analyzed; the effectiveness of current information security mechanisms in the agency has been assessed; key risks, threats, and vulnerabilities to information security under conditions of digital transformation have been identified; a set of practical recommendations has been substantiated regarding the implementation of modern cybersecurity solutions, optimization of incident management, enhancement of staff digital competence, and development of a cybersecurity culture; an economic evaluation of the proposed measures has been conducted, the integral economic effect of their implementation has been determined, and the feasibility of their adoption has been justified.

It has been concluded that the State Service of Ukraine for Transport Safety plays a key role in ensuring the protection of information flows in the field of transport security, and the level of cybersecurity of its systems directly affects the stability of infrastructure operations and public trust in government services.

The practical significance of the research results lies in the development of practical recommendations for improving the mechanisms of information security management in the public administration system under conditions of digital transformation.

The master's thesis contains 88 pages, 15 table, 10 drawings, a list of used sources from 45 names.

Keywords: information security, cybersecurity, digital transformation, public administration, cyber threats, incident management, digital competence.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДСБТ – Державна служба з безпеки на транспорті

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації України

ІБ – інформаційна безпека

НКЦК – Національний координаційний центр кібербезпеки

РНБО – Рада національної безпеки і оборони України

BCP – Business Continuity Plan (план безперервності діяльності/функціонування)

BIA – Business Impact Analysis (аналіз впливу на діяльність/функціонування)

CERT-UA - Computer Emergency Response Team of Ukraine (Команда реагування на комп'ютерні надзвичайні події України)

DLP – Data Loss Prevention (запобігання витоку даних)

DRP – Disaster Recovery Plan (план відновлення після аварії/інциденту)

EDR – Endpoint Detection and Response (захист і реагування на кінцевих пристроях)

IAM – Identity and Access Management (управління ідентичністю)

IDS – Intrusion Detection System (система виявлення вторгнень)

IOC – Indicators of Compromise (індикатори компрометації)

IPS – Intrusion Prevention System (система запобігання вторгненням)

IRP – Incident Response Plan (план реагування на інциденти)

ISMS – Information Security Management System (система управління ІБ)

KPI – Key Performance Indicators (ключові показники ефективності)

MFA – Multi-Factor Authentication (багатофакторна автентифікація)

NDR – Network Detection and Response (виявлення аномалій у мережі)

NIS2 – Network and Information Security 2 (друга версія директиви ЄС про безпеку мереж та інформаційних систем).

PAM – Privileged Access Management (керування привілейованими доступами)

RPO – Recovery Point Objective (цільова точка відновлення даних)

RTO – Recovery Time Objective (цільовий час відновлення)

SI – Security Incident (інцидент безпеки)

SIEM – Security Information and Event Management (система моніторингу та кореляції подій)

SLA – Service Level Agreement (угода про рівень надання послуг)

SOAR – Security Orchestration, Automation and Response (автоматизація реагування)

SOC – Security Operations Center (операційний центр кібербезпеки)

SOP – Standard Operating Procedure (стандартні операційні процедури)

TLS – Transport Layer Security (криптографічний протокол безпеки)

VPN – Virtual Private Network (захищений канал)

WAF – Web Application Firewall (фаєрвол веб-додатків)

XDR – Extended Detection and Response (розширене реагування, що охоплює кілька доменів)

ЗМІСТ

ВСТУП

Актуальність теми. Цифрова трансформація державного управління створює як нові можливості для підвищення ефективності управлінських процесів, так і суттєві ризики для інформаційної безпеки. Зростання обсягів електронних даних, впровадження цифрових сервісів та інтелектуальних технологій збільшують ймовірність кібератак, витоку конфіденційної інформації та порушення цілісності даних.

Особливу актуальність це питання набуває для Державної служби України з безпеки на транспорті, яка оперує великими масивами інформації щодо контролю перевезень і транспортної безпеки. Порушення захищеності інформаційних систем може призвести до збоїв у функціонуванні органу, негативно вплинути на безпеку транспортної інфраструктури та довіру громадян до державних сервісів.

Удосконалення організаційно-правових, технічних і управлінських механізмів забезпечення інформаційної безпеки є необхідною умовою стабільного та прозорого функціонування публічного управління. Дослідження сучасного стану системи захисту інформації в Укртрансбезпеці та визначення шляхів її покращення є важливим як з наукової, так і з практичної точки зору.

Проблематика інформаційної безпеки та цифрової трансформації публічного управління широко висвітлена у працях українських дослідників – М. Мінчекова, М. Нагорняка, С. Лисенка, Г. Галіпчака та інших, які аналізують концептуальні засади ІБ, нормативно-правові механізми та виклики кіберзагроз. У працях М. Засухи, Л. Сметаніної, І. Макарової та зарубіжних авторів (Y. Sun, A. Al-Ansi, T. Arifkhodzhaieva) розкриваються питання цифрової трансформації та підвищення стійкості інформаційних систем. Загалом дослідники підкреслюють необхідність комплексного, міждисциплінарного підходу до забезпечення ІБ, що підтверджує актуальність обраної теми в умовах зростання кіберзагроз.

Метою магістерської роботи є дослідження напрямів удосконалення механізмів забезпечення інформаційної безпеки в умовах цифрової

трансформації в системі публічного управління, зокрема в Державній службі України з безпеки на транспорті.

Досягнення поставленої мети передбачає вирішення таких **завдань:** розкрити сутність інформаційної безпеки в системі публічного управління, охарактеризувати вплив цифрової трансформації на формування сучасної моделі ІБ державного сектору, дослідити нормативно-правові, організаційні та управлінські механізми забезпечення інформаційної безпеки в Державній службі України з безпеки на транспорті, охарактеризувати структуру відповідальних підрозділів та проаналізувати існуючі інструменти кіберзахисту, оцінити ефективність чинних механізмів забезпечення інформаційної безпеки ДСБТ, виявити ключові ризики, загрози та вразливості інформаційній безпеці ДСБТ в умовах цифрової трансформації, обґрунтувати комплекс практичних рекомендацій щодо впровадження сучасних засобів кіберзахисту, оптимізації управління інцидентами, підвищення цифрової компетентності персоналу та розвитку культури кібергігієни, провести економічне оцінювання ефективності запропонованих заходів, визначити інтегральний економічний ефект від їх реалізації та обґрунтувати доцільність впровадження.

Об’єктом дослідження є процес забезпечення інформаційної безпеки в органах публічного управління в умовах цифрової трансформації.

Предметом дослідження є теоретичні основи, організаційні та технологічні механізми забезпечення інформаційної безпеки в системі публічного управління, а також практичні напрацювання щодо їх удосконалення в Державній службі України з безпеки на транспорті в умовах цифрової трансформації.

Методами дослідження є: загальнонаукові методи аналізу та синтезу – для вивчення теоретичних основ інформаційної безпеки та узагальнення наукових підходів; структурно-функціональний аналіз – для дослідження організаційної моделі забезпечення ІБ у ДСБТ та визначення функціональних зв’язків між підрозділами; системний підхід – для розгляду системи інформаційної безпеки як комплексного об’єкта, що поєднує управлінські,

технічні та правові компоненти; порівняльний аналіз – для зіставлення національних і міжнародних стандартів, підходів та інструментів кіберзахисту; ризик-орієнтований аналіз – для ідентифікації загроз, вразливостей та визначення рівня ризиків інформаційної безпеки; методи експертного оцінювання – для визначення ефективності чинних механізмів ІБ та обґрунтування напрямів їх удосконалення; економічний аналіз і розрахункові методи – для оцінювання економічного ефекту від запропонованих заходів і визначення їх доцільності; графічні методи – для візуалізації структури процесів та результатів аналізу; SWOT-аналіз – для виявлення сильних і слабких сторін системи інформаційної безпеки ДСБТ, а також можливостей і загроз у контексті цифрової трансформації; матричні методи (зокрема матриця пріоритетності заходів) – для обґрунтованого вибору напрямів удосконалення ІБ, визначення ресурсної важливості та черговості впровадження технічних і організаційних рішень.

Практична значущість результатів дослідження полягає у створенні практичних рекомендацій щодо вдосконалення механізмів забезпечення інформаційної безпеки в системі публічного управління в умовах цифрової трансформації, зокрема в Державної служби України з безпеки на транспорті.

Апробація. Апробація результатів наукового дослідження здійснювалася у рамках участі в роботі Міжнародної науково-практичної конференції магістрантів «Інноваційні пріоритети у розвитку економіки та менеджменту», БНАУ, 29 жовтня 2025 року, м. Б. Церква. Результати досліджень опубліковані у збірнику матеріалів конференції.

Структура кваліфікаційної роботи магістра. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг становить 88 сторінок без додатків. Список використаних джерел налічує 45 найменувань. Робота ілюстрована 10 рисунками, містить 15 таблиць.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Сутність та складові інформаційної безпеки в системі публічного управління

Інформаційна безпека (ІБ) у системі публічного управління сьогодні набуває статусу однієї з базових умов функціонування держави. Відповідно до Конституції України (стаття 17) інформаційна безпека є найважливішою функцією держави, справою всього Українського народу: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [1]. Зміст поняття інформаційної безпеки вперше системно окреслено у Законі України «Про національну безпеку України», який визначає її складову у структурі сектору безпеки і оборони та встановлює механізми державного управління цією сферою [2]. У Стратегії інформаційної безпеки наведено наступне трактування поняття «інформаційна безпека України» – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [3].

З огляду на масштаб цифрової трансформації, зростання обсягів даних, інтенсивність електронних комунікацій та загострення кіберзагроз, забезпечення захищеності інформаційних ресурсів стає не просто технологічним завданням, а стратегічною місією [4]. Для України, яка протистоїть системним та цілеспрямованим інформаційно-кібернетичним атакам, питання побудови ефективної системи ІБ в органах державної влади набуває критичного значення.

Сутність інформаційної безпеки у сфері публічного управління полягає у здатності державних інституцій забезпечувати комплексний захист інформаційних активів як технічних, так і організаційно-процесних – від загроз будь-якого походження [5, с.34]. Цей захист передбачає створення умов, за яких державні інформаційні системи здатні функціонувати безперебійно, забезпечувати достовірність та цілісність даних, протидіяти несанкціонованому доступу та гарантувати безпечний обмін інформацією між органами влади, громадянами й бізнесом.

У науковій та нормативній площині інформаційна безпека трактується багатовимірно. В українському законодавстві вона визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди шляхом використання інформаційного простору [6]. Для сфери публічного управління це поняття деталізується крізь призму захисту: державних інформаційних ресурсів, критичної інформаційної інфраструктури, систем електронного урядування, персональних даних громадян, міжвідомчих каналів комунікації, даних, що використовуються для прийняття управлінських рішень.

У цьому контексті інформаційна безпека виступає ключовим елементом державної стабільності, адже її порушення може призвести до зриву надання адміністративних послуг, компрометації державних систем, масштабних витоків даних, підриву довіри громадян та дестабілізації управління [7, с. 82].

ІБ не є суто технічним явищем. Вона охоплює: правові механізми (норми, стандарти, регламенти, політики), організаційні заходи (структура управління безпекою, відповідальні, процеси), кадрові аспекти (підготовленість персоналу,

цифрова компетентність, культура безпеки), технологічний захист (програмні й апаратні засоби, мережеві інструменти, системи контролю), процеси реагування (виявлення, знешкодження, аналіз інцидентів), управління ризиками (ідентифікація, оцінювання, мінімізація інформаційних загроз).

Тому в системі публічного управління інформаційна безпека – це синергетичне поєднання процесів, політик, технологій і людей, які мають діяти узгоджено.

Об’єктами інформаційної безпеки в публічному управлінні є [8, с. 130]:

1. Інформація різних категорій доступу: відкрита інформація, службова інформація, конфіденційна інформація, персональні дані, критична інформація, державна таємниця.

2. Інформаційні системи та електронні сервіси – електронні реєстри, системи документообігу, геоінформаційні системи, аналітичні платформи.

3. Комунікаційні мережі та канали обміну даними.

4. Технічне обладнання – сервери, робочі станції, мобільні пристрої, системи відеонагляду, обладнання віддаленого доступу.

5. Інфраструктура кіберзахисту – SIEM, SOC, DLP, IAM, системи журналювання, засоби криптозахисту.

6. Людські ресурси, включно з чиновниками, державними службовцями, технічним персоналом, адміністраторами та керівниками.

Суб’єкти інформаційної безпеки: органи державної влади, структурні підрозділи ІБ, адміністратори мереж і систем, державні службовці-користувачі, підрядники й постачальники ІТ-рішень, Національний центр кіберзахисту, ДССЗЗІ, CERT-UA, керівники органів влади (як носії управлінської відповідальності). Від якості їхньої взаємодії залежить рівень захищеності держави у кіберпросторі.

Сутність ІБ найчастіше розкривається через базові принципи CID (Confidentiality – Integrity – Availability), доповнені сучасними вимогами стійкості, підзвітності та захищеності від внутрішніх загроз [9].

1. Конфіденційність – передбачає забезпечення доступу до інформації виключно уповноважених осіб. У державному секторі це критично через:

роботу з персональними даними, обробку службової та таємної інформації, міжвідомчі документи, використання відомчих реєстрів. Засобами забезпечення є: контроль доступу, криптографія, IAM/MFA, політики ролей, сегментація мереж.

2. Цілісність – означає неможливість несанкціонованої зміни або знищення інформації. Це ключове для: державних реєстрів, фінансових документів, систем управлінської звітності, аналітичних даних для прийняття рішень. Засоби: контроль версій, резервні копії, хешування, журналювання, механізми перевірки достовірності.

3. Доступність – забезпечує безперервну роботу державних сервісів – критично важливо для: ЦНАПів, порталу «Дія», реєстрів ліцензій, дозволів, сертифікації, служб аналітичного реагування. Порушення доступності (DoS/ DDoS, збої, відмова обладнання) прямо впливають на виконання функцій держави.

4. Підзвітність та контроль дій, що передбачає: фіксацію дій користувачів, журналювання операцій, аудит доступів, можливість відслідковувати компрометацію систем.

5. Автентифікація та управління ідентичностями. У публічному управлінні це один із центральних елементів ІБ, що охоплює: електронні ключі; КЕП; багатофакторну автентифікацію; централізовані каталоги доступів; захист службових акаунтів.

6. Стійкість та відновлюваність. У сучасних умовах стійкість (resilience) означає не лише здатність захищатися, а й швидко відновлюватися. Держава має забезпечувати: резервування, дублювання сервісів, плани безперервності (BCP) і реагування (IRP), моніторинг критичних ресурсів.

Інформаційні загрози у сфері публічного управління. Державні органи є мішенню для: кібератак державного походження (APT-групи), фішингових кампаній, внутрішніх порушень (недбалість, помилки, зловживання), вразливостей в електронних реєстрах, DDoS-атак на критичні сервіси, компрометації мобільних пристроїв та віддаленого доступу, витоків даних через третіх осіб, соціальної інженерії, шкідливого ПЗ, програм-вимагачів. З кожним

роком зростає частка складних цілеспрямованих атак, що ставлять під загрозу не лише конфіденційність, а й стабільність функціонування державних інституцій.

Організаційна складова ІБ: політики, структури та відповідальність. Ефективна система ІБ у публічному управлінні передбачає наявність [10, с. 65]:

1. Політик та регламентів: політика інформаційної безпеки, політика доступів, політика паролів, політика використання пристроїв, політика резервного копіювання, політика роботи з персональними даними, політика реагування на інциденти.

2. Структур управління ІБ: підрозділи інформаційної безпеки, центри кіберзахисту (SOC), служби моніторингу, адміністратори доступів, координатори безпеки в територіальних органах.

3. Процесної моделі: управління ризиками (risk management), комплаєнс-процедури, аудит ІБ, управління інцидентами, управління вразливостями, управління змінами.

Технологічна складова інформаційної безпеки. Цифрова інфраструктура держави потребує багаторівневого технічного захисту. До ключових інструментів належать: SIEM – кореляція подій, SOC – оперативне реагування, DLP – захист від витоку, EDR/XDR – захист робочих станцій, IAM/PAM – управління ідентичностями та привілеями, VPN і шифрування трафіку, системи резервного копіювання і BCP, засоби криптографічного захисту, сканери вразливостей та патч-менеджмент [11, с. 313].

Технічні рішення створюють можливість не лише фіксувати атаки, а й передбачати їх, аналізувати тенденції загроз і формувати проактивний захист.

Кадрова складова: цифрова грамотність та культура кібергігієни. Людський фактор – ключова причина 60-80% інцидентів у державному секторі. Тому без формування культури кібергігієни неможливо створити ефективну систему ІБ. Кадрова складова включає: навчання (базові курси, ролеві програми, тренінги для керівників); симуляції фішингових атак; щотижневі інформаційні кампанії; оцінювання знань; чіткі інструкції та чеклісти; стандарти поведінки з

інформацією. Системний підхід до навчання зменшує ризик інцидентів людського фактору на 50-70% [12, с. 124].

Національна система інформаційної безпеки України має багаторівневу інституційну структуру, спрямовану на забезпечення захисту державних інформаційних ресурсів, протидію кібератакам та підтримку функціонування органів публічного адміністрування в умовах воєнного та гібридного впливу. Зрослий рівень загроз, пов'язаний з повномасштабною агресією Російської Федерації, зумовив прискорену модернізацію механізмів державного управління у сфері ІБ.

Інституційний механізм інформаційної безпеки – це особлива структурна складова частина державного механізму, що забезпечує створення норм і правил, які регулюють взаємодію різних суб'єктів в інформаційній сфері щодо запобігання загроз інформаційній безпеці [13].

Ключову координаційну роль відіграє Рада національної безпеки і оборони України (РНБО), яка формує засади національної політики кібербезпеки та інформаційного суверенітету, ухвалює стратегічні рішення щодо реагування на загрози державним інфраструктурам, у тому числі транспортній. Саме РНБО ініціювала низку рішень у 2022-2024 рр., спрямованих на посилення захисту державних реєстрів і перехід до використання державної хмари для забезпечення стійкості систем до фізичного знищення.

Центральним органом виконавчої влади у сфері технічного й криптографічного захисту інформації є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). У 2023 р. ця Служба запобігла понад 2000 масштабним кібератакам на державні ресурси, зокрема на реєстри в системі Мінінфраструктури, податкової та оборонної сфер [14]. ДССЗЗІ розробляє технічні регламенти, здійснює сертифікацію засобів захисту та координує взаємодію з приватними компаніями.

Важливим елементом системи є Національний координаційний центр кібербезпеки при РНБО (НКЦК), який виконує функції оперативного реагування на інциденти, моніторингу кіберпростору й аналізу загроз. З 2022 року діяльність НКЦК зосереджена на захисті Фонду «Дія», транспортних

систем, енергетики, фінансового сектору, а також на протидії шкідливим впливам у соціальних мережах. Центр активно співпрацює з партнерами з НАТО та ЄС у межах обміну розвідувальною інформацією.

На рівні галузевого управління кожне міністерство та центральний орган влади має власні підрозділи з кіберзахисту, зокрема Міністерство цифрової трансформації України, яке формує політику кіберстійкості державних сервісів, та відповідні підрозділи в секторі оборони й транспорту. Значного розвитку набули також CERT-UA – урядова команда реагування на комп'ютерні інциденти, яка за 2023 рік опрацювала понад 1800 кібератак різного рівня критичності.

Системоутворюючим документом у сфері ІБ є Доктрина інформаційної безпеки України, що визначає державні пріоритети: захист інформаційного суверенітету, протидія дезінформації, забезпечення кіберзахисту критичної інфраструктури, розвиток спроможностей національних сил кібероборони [15].

У 2023-2024 рр. Уряд України здійснює оновлення Доктрини з урахуванням стандартів ЄС та НАТО, нових викликів воєнного часу та необхідності інтеграції держави до спільного цифрового ринку ЄС.

Отже, державна політика інформаційної безпеки України на сучасному етапі спрямована на: централізоване управління кіберстійкістю держави, активну міжнародну співпрацю у сфері кібероборони, впровадження європейських та натівських стандартів, захист персональних даних та безпеки громадян, зміцнення готовності публічного управління до кібератак.

1.2 Цифрова трансформація як чинник змін у сфері інформаційної безпеки

Цифрова трансформація – це комплексний процес інтеграції цифрових технологій у всі сфери функціонування держави, економіки та суспільства, що передбачає зміну моделей управління, оптимізацію бізнес-процесів і підвищення якості публічних послуг шляхом впровадження інноваційних технологічних рішень та переходу до клієнтоорієнтованої логіки діяльності

державних інституцій [16, с. 98]. Її ключовою метою є створення нової цінності через цифрові інструменти, забезпечення прозорості та підзвітності влади, а також зміцнення національної безпеки, включно з інформаційною та кібербезпекою.

Цифрова трансформація публічного сектору є ключовим напрямом модернізації системи публічного управління України. У межах цього процесу інформація перетворюється на стратегічний ресурс, а цифрові технології – на основний інструмент державного управління [17]. Водночас зростає залежність держави від стійкості цифрового середовища й надійності механізмів інформаційної безпеки. В умовах воєнного стану цей фактор стає визначальним для забезпечення суверенітету та управлінської безперервності.

Цифровізація публічного адміністрування в Україні виступає провідним чинником еволюції системи інформаційної безпеки держави. Так, концепція «держава як сервіс» є еволюцією моделі електронного урядування, і точна дата її появи не фіксується одним документом. Однак можна виділити етапи впровадження у світі та в Україні: Упровадження концепції пов’язане з цифровою реформою державного управління, яка активізувалася після 2019 року (таблиця 1.1).

Таблиця 1.1

Етапи впровадження концепції «держава як сервіс» в Україні

Рік	Подія
2019	Створення Міністерства цифрової трансформації України та публічне проголошення курсу на модель «держава як сервіс»
2020	Запуск застосунку й порталу «Дія» → початок масштабної автоматизації послуг
2021-2022	Законодавче розширення електронних сервісів, цифрові документи
2023-2024	Інтеграція реєстрів, хмарні рішення, кіберпосилення держави в умовах війни

Тобто в Україні концепція де-факто почала реалізовуватися у 2019 році та стала ключовою платформою цифрової трансформації публічного адміністрування. У межах концепції «держава як сервіс» здійснюється глибока трансформація управлінських процесів, яка охоплює автоматизацію адміністративних процедур, розвиток електронної взаємодії між органами

влади, перехід до електронного документообігу та широке впровадження цифрових сервісів для громадян і бізнесу. Важливим напрямом цифрової модернізації є також створення єдиного простору державних інформаційних ресурсів, що забезпечує інтегрованість реєстрів і оперативний обмін даними між різними суб'єктами публічного управління [18].

Реалізація зазначених підходів сприяє посиленню інформаційної безпеки, оскільки автоматизація процесів значно зменшує вплив людського фактора та імовірність внутрішніх порушень. У той самий час запровадження засобів електронної ідентифікації та багаторівневої автентифікації дозволяє забезпечити належний контроль доступів до даних і державних інформаційних систем. Важливу роль відіграє цифровий аудит, що забезпечує простежуваність та підзвітність дій уповноважених осіб, сприяє виявленню шахрайських операцій і удосконаленню внутрішніх процесів на основі об'єктивного аналізу.

Разом з тим зростання цифрової залежності державного сектору формує новий контур ризиків та вимоги до гарантованої кіберстійкості. Чим інтенсивніше розвивається електронне врядування, тим більше життєво важливі функції держави залежать від безперервної роботи інформаційно-комунікаційних систем, захисту їх від зовнішніх атак, технічних збоїв чи внутрішніх загроз [19]. Таким чином, цифровізація виступає подвійним чинником: з одного боку, посилює спроможність держави забезпечувати інформаційну безпеку, а з іншого – загострює потребу у формуванні комплексної, надійної та адаптивної системи кіберзахисту.

Стрімка цифровізація публічного управління зумовлює необхідність переосмислення традиційних механізмів забезпечення інформаційної безпеки та адаптації їх до нових технологічних реалій. Зміни відбуваються комплексно – на організаційному, правовому, технічному, кадровому та комунікаційному рівнях, формуючи сучасну модель захисту державних інформаційних ресурсів, що відповідає стандартам Європейського Союзу та вимогам національної безпеки (таблиця 1.2).

Таблиця 1.2

Вплив цифрової трансформації на складові інформаційної безпеки в системі публічного управління

№	Складова інформаційної безпеки	Зміст трансформаційних змін	Значення для забезпечення ІБ
1	Організаційні механізми	Формування державної системи управління кібербезпекою; створення структур реагування на інциденти; розвиток міжвідомчої цифрової взаємодії; перехід від реактивного до проактивного ризик-менеджменту	Підвищення готовності держави до прогнозування та запобігання кіберзагрозам; скорочення часу реагування на інциденти
2	Правове забезпечення	Гармонізація законодавства з європейськими стандартами (GDPR, NIS2, eIDAS); впровадження принципу «безпека за замовчуванням і за дизайном»; посилення відповідальності за порушення захисту даних	Підвищення рівня правового захисту інформації; розширення гарантій безпеки персональних та службових даних
3	Технічні інструменти	Використання хмарних технологій, біометричної автентифікації, розподілених реєстрів; впровадження систем виявлення вторгнень, протидія DDoS-атакам; розвиток криптографічного захисту	Перехід до комплексного кіберзахисту та цифрової стійкості державних інформаційних систем
4	Кадрова підготовка та культура кібербезпеки	Підвищення вимог до компетентностей персоналу; підготовка аналітиків загроз, IT-аудиторів; включення модулів з кібергігієни до програм навчання держслужбовців	Зниження ризику внутрішніх порушень, формування професійної спроможності органів влади у сфері ІБ
5	Комунікаційні механізми захисту	Посилення захисту інформаційних каналів від дезінформації; розвиток медіастійкості суспільства; інформаційно-аналітичний моніторинг інформаційних атак	Зменшення впливу інформаційно-психологічних операцій, підвищення рівня довіри громадян до держави

Таким чином, цифрова трансформація виступає ключовим вектором розвитку системи інформаційної безпеки, оскільки охоплює не лише технічні аспекти захисту, а й трансформує управлінську модель, правове середовище, кадрову політику та інформаційні комунікації держави. Це забезпечує формування сучасної кіберстійкої архітектури публічного адміністрування, здатної ефективно протистояти гібридним загрозам.

Стрімкий розвиток цифрових технологій та їх масове впровадження в публічному адмініструванні не лише створюють нові можливості для

ефективного управління, а й формують якісно нові загрози інформаційній безпеці держави. За останні роки характер ризиків змінився від локальних технічних інцидентів до масштабних комплексних атак, спрямованих на підрив управлінської спроможності, порушення доступності критичних послуг та інформаційний вплив на суспільство. У цьому контексті важливо класифікувати сучасні загрози, що виникають у цифровому середовищі публічної влади.

Цифрова трансформація трансформує систему інформаційної безпеки за двома напрямами [20, с. 74]:

- створює нові можливості для захисту інформаційних процесів (таблиця);
- породжує нові ризики і загрози, пов’язані з кіберпростором.

Розглянемо позитивний вплив цифрової трансформації на ІБ. В таблиці 1.3 наведено позитивний вплив цифрової трансформації на систему інформаційної безпеки в публічному управлінні.

Таблиця 1.3

Позитивний вплив цифрової трансформації на систему інформаційної безпеки в публічному управлінні

№	Напрям впливу цифрової трансформації	Сутність змін і результати	Значення для інформаційної безпеки
1	Підвищення стійкості систем управління	Запровадження технологій резервного копіювання та дублювання функцій органів влади	Забезпечення неперервності державного управління навіть у разі кібератак чи руйнування інфраструктури
2	Зниження корупційних ризиків	Автоматизація процедур, мінімізація людського фактору при ухваленні рішень	Унеможливлення маніпуляцій із даними, прозорість процесів контролю
3	Розвиток аналітики безпеки	Використання Big Data та ШІ для виявлення аномалій і прогнозування загроз	Превентивне реагування на кіберінциденти, посилення проактивного захисту
4	Оперативність реагування на інциденти	Цілодобова робота кіберцентрів моніторингу, автоматизовані сповіщення та ізоляція інцидентів	Зменшення масштабів наслідків порушень, прискорення відновлення функцій
5	Прозорість і підзвітність держави	Публічність рішень, електронні реєстри, аудит цифрових дій службовців	Зростання довіри громадян і зниження інформаційних маніпуляцій
6	Використання державної хмари	Централізоване, географічно розподілене зберігання критичних даних	Захист інформації навіть у разі фізичного знищення об’єктів ІТ-інфраструктури

Отже, цифрова трансформація суттєво підвищує рівень інформаційної безпеки в системі публічного адміністрування завдяки зміцненню стійкості державних інформаційних ресурсів, автоматизації процесів контролю доступу та впровадженню аналітичних інструментів виявлення загроз.

Інтеграція штучного інтелекту, великих даних і сучасних систем моніторингу забезпечує проактивне реагування на кіберінциденти та мінімізацію людського фактору, який є одним із найбільш ризикових елементів у сфері ІБ. При цьому створення державної хмари гарантує збереження критичних даних навіть за умов фізичного ураження інфраструктури, що є особливо актуальним в умовах воєнного стану [21, с. 35].

Таким чином, цифровізація виступає не лише каталізатором змін у діяльності органів влади, але й фактором зміцнення інформаційного суверенітету та загальної стійкості держави до гібридних загроз.

В таблиці 1.4 наведено сучасні загрози інформаційній безпеці в умовах цифровізації публічного управління.

Таблиця 1.4

Сучасні загрози інформаційній безпеці в умовах цифровізації публічного управління

№	Категорія загрози	Сутність загрози	Потенційні наслідки для держави та суспільства
1	Кібератаки на державні інформаційні системи	Несанкціоноване втручання в роботу ІКС, шкідливе програмне забезпечення, DDoS-атаки, порушення доступності сервісів	Паралізація функцій органів влади, недоступність державних послуг, втрата оперативного управління
2	Інсайдерські загрози	Зловживання доступами або помилки персоналу, витік конфіденційних даних, навмисні чи ненавмисні порушення	Компрометація реєстрів і службової інформації, зростання корупційних ризиків
3	Атаки на критичну інфраструктуру	Порушення роботи транспортної, енергетичної, фінансової систем через втручання в інформаційні технології	Загроза життю населення, збої в економіці, зниження обороноздатності держави
4	Витоки та незаконний обіг персональних даних	Кіберкрадіжки баз даних, підробка цифрової ідентичності, маніпулювання доступами	Порушення прав громадян, дискредитація органів влади, штрафи й міжнародна відповідальність

5	Дезінформаційні та інформаційно-психологічні операції	Вплив на громадську думку, поширення маніпулятивного контенту, підробка офіційної інформації	Підрив довіри до влади, соціальна дестабілізація, послаблення здатності держави приймати рішення
6	Збої та залежність від зовнішніх цифрових платформ	Відмова або недоступність комерційних сервісів, на яких базуються державні ІТ-рішення	Втрата контролю над даними, ризик блокування критичних сервісів
7	Автоматизовані та AI-генеровані атаки	Використання ШІ для злому, створення фішингових схем, deepfake-технології	Ускладнення верифікації інформації, прискорення кіберзагроз
8	Кібершпигунство держав-агресорів	Викрадення стратегічних даних, проникнення в захищені системи	Загроза національній безпеці, компрометація оборонних операцій

Повномасштабна агресія проти України значно підвищила інтенсивність та складність загроз інформаційній безпеці. Українські державні системи щоденно зазнають кібератак, спрямованих на порушення управлінських процесів, компрометацію критичних даних і дестабілізацію суспільства через інформаційний вплив [22]. У цих умовах кіберзахист і стійкість до інформаційних впливів стають невід'ємними елементами гарантування національної безпеки і функціонування органів публічної влади.

Цифровізація державного управління потребує формування сучасної системи інформаційної безпеки, що ґрунтується на визначених принципах [23]. Вони забезпечують ефективність, узгодженість і стійкість захисних заходів у сфері публічного адміністрування.

1. Принцип комплексності передбачає, що забезпечення інформаційної безпеки має здійснюватися на всіх рівнях управління та охоплювати:

правовий рівень – чітке регулювання режимів доступу й відповідальності;

організаційний рівень – регламенти, структурні підрозділи ІБ, контроль доступів;

технічний рівень – криптографія, системи кіберзахисту, резервування даних;

кадровий рівень – навчання, сертифікація персоналу, розмежування повноважень.

Комплексність означає, що жоден із цих елементів не може забезпечити захист окремо, а їх синергія гарантує максимальну стійкість державних

інформаційних ресурсів. Захист має бути інтегрованим у всі управлінські процеси – від розроблення політик до їх практичної реалізації.

2. Принцип безперервності орієнтує систему ІБ на постійне: виявлення кіберзагроз, оновлення засобів захисту, аудит стану інформаційних систем, реагування на інциденти. Завдяки цьому механізми ІБ не залишаються статичними, а адаптуються до еволюції загроз, які швидко змінюються. Безперервність включає: моніторинг у реальному часі, аналітику та прогнозування атак, своєчасне усунення вразливостей. Таким чином, система ІБ працює превентивно, а не лише у відповідь на події.

3. Принцип ризик-орієнтованості – сучасна модель ІБ передбачає розстановку пріоритетів на основі аналізу ризиків, оскільки ресурси держави не є безмежними. Це означає: ідентифікацію найбільш цінних інформаційних активів; визначення ймовірності загроз і рівня можливих збитків; пріоритизацію заходів захисту; застосування пропорційних заходів безпеки.

Захищати потрібно перш за все те, що має найбільший вплив на національну безпеку та права громадян: критична інфраструктура, реєстри, персональні дані. Захист має бути не максимальним, а оптимально достатнім.

4. Принцип інтеграції передбачає , що інформаційна безпека має діяти не фрагментарно, а у спільному цифровому просторі держави. Це передбачає: єдині стандарти захисту в органах влади, сумісність інформаційних систем, централізовану координацію кіберзахисту, обмін інцидентами й аналітикою між установами. Інтеграція дає змогу швидше реагувати на загрози, уникати дублювання функцій та досягати єдиних високих стандартів управління інформаційною безпекою в державному секторі.

5. Принцип сталості та відмовостійкості передбачає: здатність державних систем функціонувати безперервно навіть під час кризових подій – кібератак, збоїв, воєнних дій; збереження доступу до критичних даних; відновлення роботи систем у короткі терміни. Основні інструменти реалізації: багаторівневе резервування, географічно розподілені дата-центри, державні хмарні технології, кіберзаходи у воєнних умовах. У центрі цього принципу – стійкість держави до цифрових деструктивних впливів.

Ці принципи: формують цілісну концепцію сучасної інформаційної безпеки враховують специфіку цифрового середовища та воєнних загроз в Україні, слугують основою для державної політики у сфері захисту інформаційних ресурсів

У процесі цифрової трансформації відбувається істотна зміна ролі держави в системі забезпечення інформаційної безпеки. Якщо раніше основним завданням держави був переважно захист інформаційних ресурсів від зовнішніх посягань, то нині вона виступає архітектором цифрового середовища, створюючи та підтримуючи комплексні інформаційні екосистеми для надання публічних послуг. Держава також набуває функцій оператора та власника критично важливих даних, від безпеки яких безпосередньо залежить стабільність управлінських процесів і захист прав громадян [25].

Окрім того, сучасна держава виконує роль модератора інформаційного простору, забезпечуючи його захищеність від деструктивних інформаційних впливів, зокрема в умовах гібридної війни. Зміцнення кіберспроможності державних інституцій зумовлює посилення їхньої позиції як активного суб'єкта кібероборони, здатного запобігати, виявляти та нейтралізовувати загрози національній безпеці у цифровій сфері.

Таким чином, інформаційна безпека з допоміжної функції перетворюється на стратегічний пріоритет публічного управління, що визначає ефективність і стійкість державного управління в умовах цифрової трансформації.

Цифрова трансформація виступає потужним драйвером розвитку системи інформаційної безпеки в Україні, забезпечуючи модернізацію технічної інфраструктури, удосконалення правового регулювання та підвищення ефективності управління. Водночас цифровізація актуалізує нові загрози, передусім пов'язані з кібератаками та інформаційним впливом на суспільство, що вимагає формування комплексної, адаптивної, ризик-орієнтованої системи ІБ. В умовах воєнного стану кіберстійкість і безперервність управління набувають критичного значення, забезпечуючи захист державного суверенітету й довіру громадян до органів публічного адміністрування.

Висновки до розділу 1:

Отже, інформаційна безпека є багатовимірною категорією, яка охоплює правові, організаційні, технічні, кадрові та комунікаційні складові. Вона забезпечує цілісність, конфіденційність, доступність і стійкість державних даних, а також формує підзвітність і керованість інформаційних процесів у публічному секторі. Визначено, що об'єктами ІБ виступають як інформаційні системи та мережі, так і людські ресурси, а суб'єктами – широке коло державних органів та центрів кіберзахисту, включаючи ДССЗЗІ, НКЦК та CERT-UA. Національна модель ІБ функціонує у контексті міжнародних стандартів (ISO/IEC 27001, NIS2, GDPR), що забезпечує її адаптивність до глобальних викликів.

У підрозділі 1.2 підкреслено, що цифрова трансформація є ключовим чинником зміни архітектури інформаційної безпеки. Зростання цифрових сервісів, інтеграція державних реєстрів, автоматизація управлінських процесів і розвиток електронної взаємодії посилюють роль ІБ як складової національної безпеки. Водночас цифровізація створює новий контур ризиків – від кібератак та інсайдерських загроз до інформаційно-психологічних операцій і витоків персональних даних. Це потребує переходу від фрагментарних заходів до системної, ризик-орієнтованої моделі кіберзахисту, заснованої на проактивному моніторингу, хмарних технологіях, багаторівневій автентифікації та інтегрованих SOC/SIEM-рішеннях.

Узагальнюючи, у розділі доведено, що сучасна система інформаційної безпеки в публічному управлінні повинна базуватися на принципах комплексності, безперервності, інтеграції, ризик-орієнтованості та відмовостійкості. Зміна ролі держави від споживача ІТ-рішень до архітектора цифрового середовища вимагає нової управлінської логіки, де ІБ виступає не додатковою функцією, а фундаментом сталого та безпечного функціонування держави. В умовах воєнного стану ці принципи набувають критичної ваги, адже забезпечують захист національного суверенітету, стабільність державних процесів і довіру громадян до цифрової інфраструктури.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДСБТ У КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

2.1 Організаційно-управлінські засади управління інформаційною безпекою в ДСБТ

Державна служба України з безпеки на транспорті (Укртрансбезпека) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Віце-прем'єр-міністра з відновлення України – Міністра розвитку громад, територій та інфраструктури і який реалізує державну політику у сфері безпеки на автомобільному транспорті загального користування, міському електричному та залізничному транспорті. ДСБТ утворена 10 вересня 2014 р. Постановою Кабінету Міністрів № 442 шляхом злиття Державної інспекції з безпеки на морському та річковому транспорті, Державної інспекції з безпеки на наземному транспорті. Цій же Службі було підпорядковано Державну спеціальну службу транспорту. Положення про Державну службу України з безпеки на транспорті було затверджене 11 лютого 2015 року. Укртрансбезпека здійснює свої повноваження безпосередньо, через утворені в установленому порядку територіальні органи та Держспецтрансслужбу.

Організаційна структура ДСБТ побудована за функціонально-ієрархічним принципом та включає керівництво, центральний апарат, територіальні управління в областях України і спеціалізовані структурні підрозділи, відповідальні за окремі напрями державного контролю, цифровізації, кадрової політики, фінансового забезпечення тощо. Станом на 2024 рік гранична чисельність працівників становила 813 штатних одиниць, з яких 296 – державні службовці.

1. Керівництво координує діяльність підрозділів за напрямами – адміністративна діяльність, нагляд і контроль, цифровізація, правова політика,

фінансово-економічне забезпечення, робота з персоналом. Підпорядкування керівництва ДСБТ зображено на рисунку 2.1.

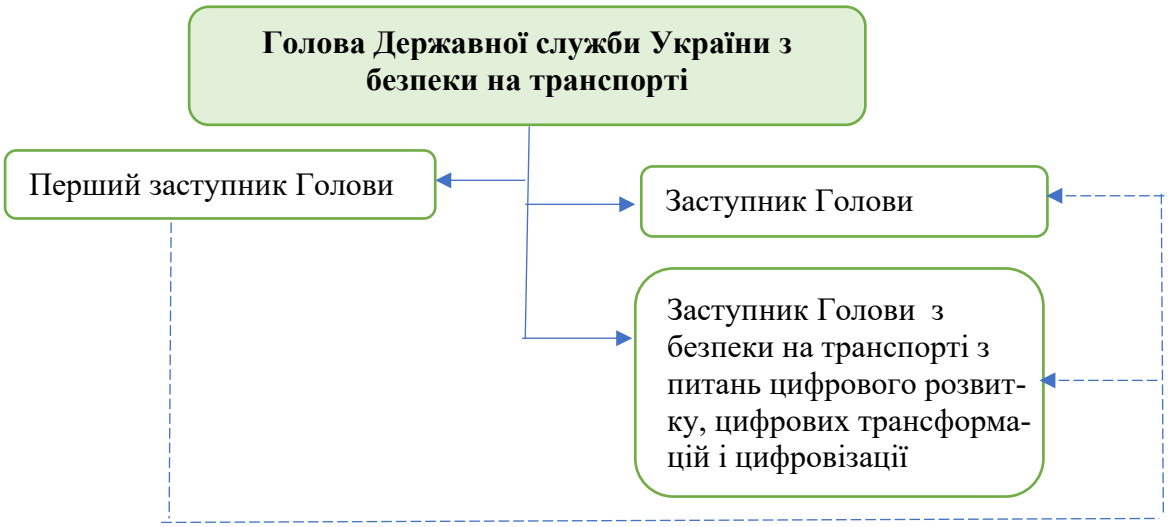

Рис. 2.1. Організаційно-управлінська структура керівництва Державної служби України з безпеки на транспорті

2. Центральний апарат ДСБТ – це основна управлінська ланка служби, яка забезпечує організацію, координацію, планування та контроль діяльності всієї системи органів Укртрансбезпеки, включно з територіальними управліннями.

Центральний апарат ДСБТ виконує функції інтелектуального та координаційного центру служби, що забезпечує формування та реалізацію державної політики у сфері транспортної безпеки, управління інформаційними ресурсами, цифрову трансформацію та кіберзахист, а також ефективну взаємодію з урядовими структурами й громадськістю (таблиця 2.1). Склад структурних підрозділів центрального апарату відображено в додатку А.

3. Територіальні органи. ДСБТ має територіальні управління (відділи) в усіх областях України, які здійснюють: контроль за дотриманням законодавства у сфері транспортних перевезень; моніторинг безпеки руху; ведення адміністративної практики (накладення штрафів, розгляд справ); роботу з перевізниками та суб’єктами господарювання на регіональному рівні.Кожен територіальний підрозділ очолює начальник управління державного нагляду (контролю) у відповідній області.

Таблиця 2.1

Призначення, функції та результати діяльності центрального апарату ДСБТ

Напрям діяльності	Основні функції центрального апарату	Очікувані результати / ефекти
1. Реалізація державної політики у сфері транспортної безпеки	Розроблення проєктів нормативно-правових актів. Формування та реалізація державних програм безпеки перевезень. Узгодження політики з Мінвідновлення та іншими органами.	Єдина державна політика у сфері транспортної безпеки. Підвищення ефективності регулювання та контролю.
2. Управління діяльністю територіальних органів	Координація регіональних управлінь. Моніторинг показників діяльності та виконання планів державного контролю. Методична підтримка та навчання персоналу.	Узгоджені дії територіальних структур. Підвищення якості контролю на місцях.
3. Нормативно-правове та організаційне забезпечення	Розробка внутрішніх регламентів, положень, наказів. Правова експертиза рішень служби. Організація правового супроводу контрольних заходів.	Уніфікована правова база діяльності служби. Зниження кількості правових помилок і спорів.
4. Цифрова трансформація та автоматизація	Впровадження ЄКІС, HRMIS, SIEM. Адміністрування електронних сервісів і реєстрів. Координація з Мінцифрою, Держспецзв’язку.	Автоматизація державних послуг. Прозорість і зручність взаємодії з громадянами.
5. Кіберзахист та інформаційна безпека	Забезпечення КСЗІ. Криптографічний захист інформації. Моніторинг інцидентів і реагування на загрози.	Підвищення захисту державних даних. Стійкість ІТ-інфраструктури до кібератак.
6. Управління персоналом	Підбір, навчання, атестація держслужбовців. Розробка політик мотивації та розвитку кадрів.	Підвищення професійного рівня персоналу. Формування етичної та доброчесної культури служби.
7. Внутрішній контроль і аудит	Проведення внутрішніх перевірок і аудитів. Аналіз ефективності управлінських рішень. Моніторинг фінансової дисципліни.	Зниження ризиків порушень і зловживань. Підвищення довіри до діяльності служби.
8. Комунікація та зв’язки з громадськістю	Інформаційна політика, публічні звіти, робота зі ЗМІ. Прийом звернень громадян.	Відкритість і прозорість діяльності служби. Зростання довіри суспільства до ДСБТ.

Організаційно-управлінська структура ДСБТ забезпечує функціональний поділ відповідальності, прозорість управління та контроль за безпекою на

транспорті. У процесі цифрової трансформації акцент робиться на підрозділах, що відповідають за ІТ-інфраструктуру, аналітику, моніторинг і кібербезпеку, які стають ключовими елементами нової управлінської моделі.

ДСБТ виконує функції: державного нагляду (контролю) за дотриманням законодавства у сфері безпеки перевезень; ліцензування діяльності перевізників;державного ринкового нагляду за технічними регламентами транспортної продукції; організації міжнародних і внутрішніх перевезень (видача дозволів, контроль за маршрутом, сертифікація); ведення електронних реєстрів (Єдиний реєстр маршрутів, ЄКІС Укртрансбезпеки тощо); розслідування аварій та інцидентів на наземному транспорті.

Протягом 2024 року було проведено понад 270 позапланових заходів державного контролю, за результатами яких до державного бюджету надійшло понад 438 млн грн штрафів.

В умовах воєнного стану ДСБТ активно переходить до електронного управління – у 2024 році реалізовано: впровадження HRMIS (системи управління людськими ресурсами в державних органах); запуск електронних реєстрів автобусних маршрутів та дозволів; розроблення модулів інтеграції з Єдиною судовою інформаційною системою («Е-суд»); розроблення технічного завдання до модернізації Єдиного комплексу інформаційних систем Укртрансбезпеки (ЄКІС); інтеграція з системою «Трембіта» для обміну даними з іншими державними реєстрами.

Кадрова політика базується на принципах відкритого добору, професійного розвитку та доброчесності. Протягом 2024 року 93% державних службовців підвищили кваліфікацію, а понад 60% пройшли навчання з кіберзахисту, права ЄС та антикорупційних стандартів. Впроваджено Кодекс етичних норм і проєкт «Будинок доброчесності» у партнерстві з програмою U-LEAD з Європою.

Організаційно-управлінські засади діяльності ДСБТ у 2024-2025 роках характеризуються поступовим переходом від традиційної вертикально-бюрократичної моделі до цифрової, прозорої, орієнтованої на результат системи управління.

Тепер детальніше розглянемо особливості управління інформаційною безпекою в ДСБТ.

Управління інформаційної безпеки є структурним підрозділом центрального апарату Державної служби безпеки на транспорті, уповноваженим на формування, реалізацію та контроль дотримання політики інформаційної безпеки. Підрозділ забезпечує стійкість інформаційно-комунікаційних систем, а також захист державних інформаційних ресурсів і даних, що обробляються в процесі діяльності служби. виконує функції ключового елемента системи управління ризиками у цифровому середовищі. Його діяльність спрямована на створення й підтримання безпечного, надійного та стійкого інформаційного простору служби, який відповідає вимогам національного законодавства та міжнародним стандартам у сфері кіберзахисту.

Основна мета Управління – створення комплексної системи інформаційної безпеки (КСЗІ) ДСБТ, яка гарантує цілісність, доступність, конфіденційність та захищеність інформації у процесі функціонування цифрових сервісів і державних реєстрів, що використовуються в діяльності служби.

Основні завдання Управління: розроблення та впровадження стратегії інформаційної безпеки ДСБТ відповідно до вимог законодавства України, актів Держспецзв'язку, Мінвідновлення та міжнародних стандартів (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR); організація моніторингу, аналізу та реагування на інциденти інформаційної безпеки; забезпечення захисту критичної інформаційної інфраструктури (КІІ) у сфері транспортної безпеки; координація заходів з кіберзахисту, взаємодія з Держспецзв'язку, CERT-UA, СБУ, Мінцифрою; розробка політик управління ризиками у сфері ІБ; проведення внутрішніх аудитів, тестувань та навчань персоналу з питань інформаційної безпеки.

Структура Управління інформаційної безпеки:

1. Відділ інформаційної безпеки. Основні функції: розроблення, впровадження та актуалізація політик, стандартів і процедур інформаційної безпеки, захист інформаційних активів, включно з управлінням доступом та контролем прав користувачів, моніторинг подій інформаційної безпеки та

виявлення інцидентів, аналіз і документування інцидентів, координація реагування та взаємодія зі спеціалізованими державними органами, проведення внутрішніх аудитів і перевірок відповідності вимогам ІБ, оцінка ризиків інформаційної безпеки та розроблення заходів їх мінімізації, організація навчання, тренінгів та підвищення кіберобізнаності персоналу.

Ключові напрями діяльності: провадження міжнародних стандартів та практик (ISO/IEC 27001, NIST CSF, GDPR), розвиток та підтримка системи управління інформаційною безпекою (СУІБ), підсилення процесів моніторингу та реагування (SOC/SIEM-підходи), централізоване управління засобами технічного захисту інформації, формування культури кібербезпеки в організації.

2. Відділ критичної інфраструктури. Основні функції: ідентифікація, категоризація та облік об’єктів критичної інформаційної інфраструктури у сфері транспортної безпеки, формування та ведення реєстру об’єктів критичної інфраструктури, аналіз загроз, оцінка ризиків та визначення рівня стійкості КІ, організація захисту технологічних систем, ключових сервісів і транспортних процесів, моніторинг стану кіберзахисту об’єктів критичної інфраструктури, контроль дотримання нормативних вимог та стандартів щодо КІ, взаємодія з Держспецзв’язку, CERT-UA, СБУ та іншими органами щодо інцидентів, що стосуються КІ, координація реагування на кіберінциденти, що впливають на критичні процеси.

Ключові напрями діяльності: забезпечення кіберстійкості критичних процесів та об’єктів транспортної сфери, реалізація вимог законодавства щодо захисту критичної інфраструктури, розроблення та впровадження планів забезпечення безперервності та відновлення роботи КІ після інцидентів, впровадження сучасних технічних засобів кіберзахисту для критичних систем, організація оперативного обміну інформацією про загрози та інциденти з державними органами.

Управління інформаційної безпеки тісно співпрацює з: управлінням цифрової трансформації, юридичним департаментом, департаментом внутрішнього моніторингу, ДССЗЗі, CERT-UA; НКЦК при РНБО (рис. 2.2).

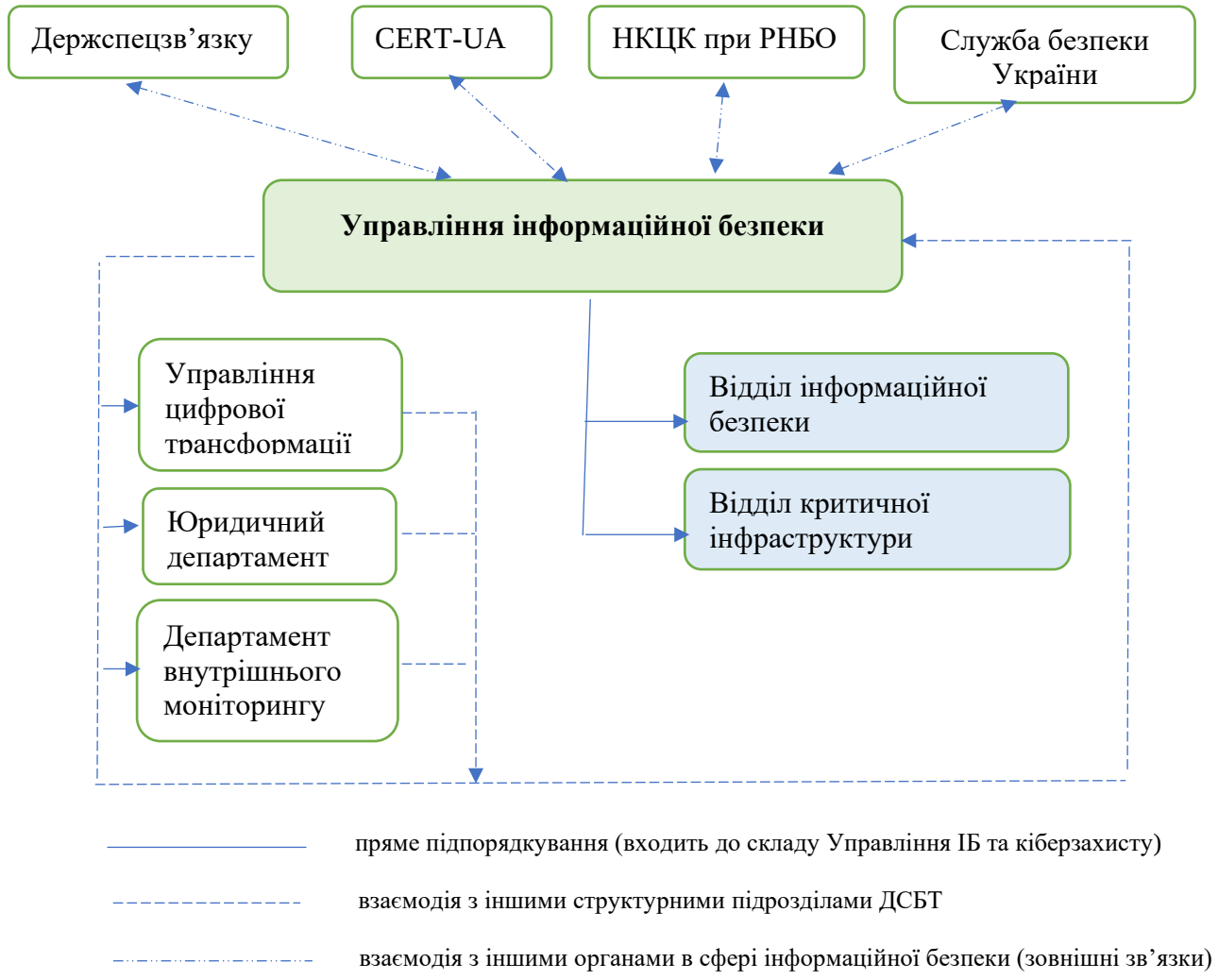

Рис.2.2. Організаційна структура та взаємодія підрозділів ДСБТ у сфері інформаційної безпеки

Така модель дозволяє забезпечити комплексний підхід до виявлення, реагування та запобігання кіберзагрозам у діяльності ДСБТ.

2.2. Оцінка ефективності чинних управлінських механізмів забезпечення інформаційної безпеки в ДСБТ

Оцінка ефективності управлінських механізмів забезпечення інформаційної безпеки в ДСБТ є одним із визначальних етапів у процесі формування системи захисту критично важливих інформаційних ресурсів та підтримання безперервності функціонування організаційних структур служби.

Ключові аспекти оцінки: аналіз нормативно-правової бази, оцінка впроваджених механізмів, оцінка ефективності реагування на інциденти, оцінка

кадрового забезпечення. Методи оцінки: аудит, тестування на проникнення, опитування та інтерв'ю, аналіз інцидентів.

Здійснимо аналіз нормативно-правового забезпечення з позиції оцінки ефективності управлінських механізмів ІБ у ДСБТ:

1.1 Законодавча база. ДСБТ у сфері ІБ спирається на загальнодержавні акти, порядки, інструкції, стандарти і т.д. (рис. 2.3).

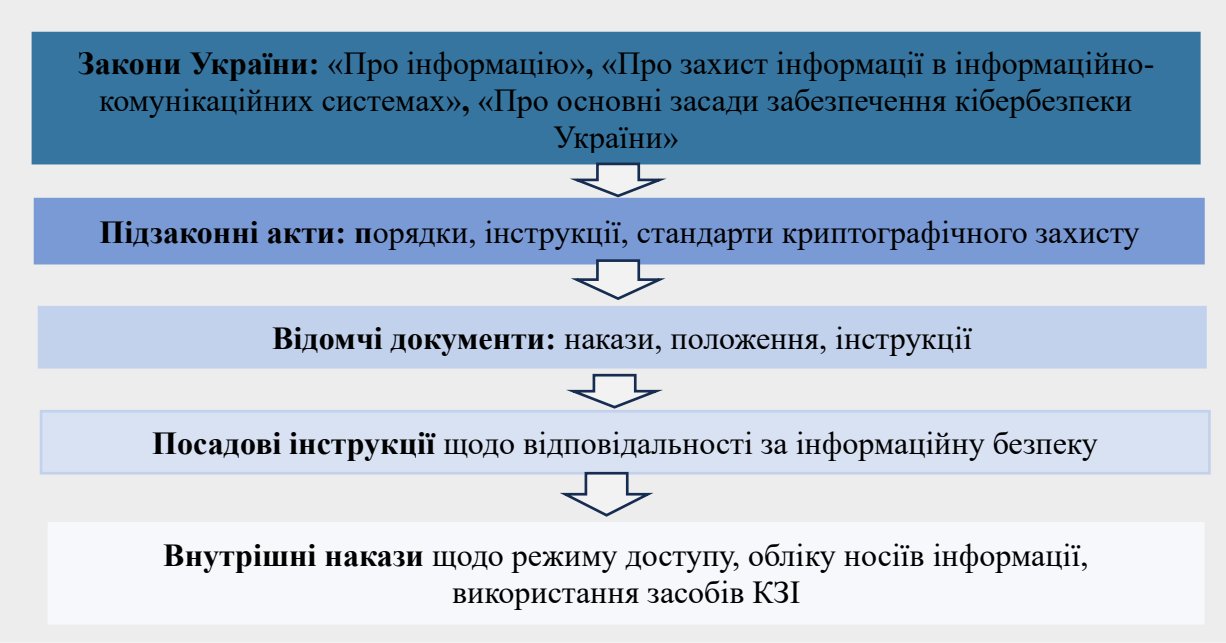

Рис. 2.3. Ієрархія нормативно-правового забезпечення ІБ у ДСБТ

Оцінка ефективності: нормативна база є; забезпечує відповідність національним вимогам; немає єдиної внутрішньої галузевої політики для ДСБТ, адаптованої під специфіку транспортної безпеки; частково відстає від міжнародних стандартів (ISO/IEC 27001, NIST).

1.2. Відомчі документи та внутрішні регламенти: існують посадові інструкції щодо відповідальності за захисту інформації; діють внутрішні накази та положення щодо режиму доступу, обліку носіїв інформації, використання КЗІ. Оцінка ефективності: формалізована відповідальність посадових осіб; контроль доступу та порядок роботи з інформацією; слабка інтеграція ризик-менеджменту; регламенти часто носять формальний характер і не містять механізмів моніторингу/звітності.

1.3. Контроль і аудит: планові перевірки проводяться відповідно до нормативів Держспецзв'язку; здійснюється контроль використання сертифікованих засобів захисту. Оцінка ефективності: перевірки забезпечують мінімальний рівень дотримання вимог; аудит здебільшого перевіряє формальну наявність документів, а не їхню практичну дієвість; відсутність регулярних незалежних аудитів за міжнародними практиками.

1.4. Відповідність міжнародним стандартам: частково застосовуються принципи ISO/IEC 27001 (класифікація даних, контроль доступів), але відсутня сертифікація; політики конфіденційності та захисту персональних даних ще не повністю відповідають GDPR та ISO/IEC 27701. Оцінка ефективності: невідповідність сучасним європейським вимогам; ризики у контексті інтеграції України в ЄС.

Отже, нормативно-правове забезпечення в ДСБТ забезпечує лише базовий рівень захисту інформації для формальної відповідності законодавству, водночас характеризується низькою адаптивністю до нових загроз і міжнародних вимог та обмежено підтримує управлінські механізми через відсутність комплексних політик ризик-менеджменту, безперервності діяльності й інтегрованої системи управління інформаційною безпекою. Таким чином, ефективність можна оцінити як середню, із сильним акцентом на формальне дотримання вимог, але слабкою практичною імплементацією.

2. Організаційні механізми забезпечення інформаційної безпеки в ДСБТ – це сукупність структур, процесів та управлінських рішень, спрямованих на підтримку належного рівня інформаційної безпеки у відомстві.

2.1. Структура управління інформаційною безпекою. У ДСБТ визначено підрозділи/відповідальних осіб за ІБ. Є посадові інструкції, що встановлюють відповідальність персоналу. Оцінка ефективності: наявність формалізованої відповідальності; обмежена кількість фахівців із ІБ.

2.2. Політики та регламенти – створюють базову систему контролю; носять переважно формальний характер, часто застосовуються лише в межах перевірок; слабка інтеграція з ризик-менеджментом і плануванням безперервності діяльності (BCP/DRP).

2.3. Кадрова та освітня політика. Працівники ознайомлюються з вимогами ІБ при прийомі на роботу також проводяться окремі інструктажі. Оцінка ефективності: мінімальний рівень обізнаності персоналу забезпечується; немає системної культури кібербезпеки серед всіх співробітників.

2.4. Контроль та аудит. Перевірки здійснюються планово, фіксуються порушення та видаються накази щодо їх усунення. Контроль існує, але часто формалізований; немає внутрішнього проактивного моніторингу інцидентів; аудит не завжди передбачає оцінку реальних ризиків.

Загальна оцінка організаційного механізму ДСБТ у сфері ІБ: забезпечує формальну відповідність законодавству, створює мінімальні умови для контролю доступу та відповідальності персоналу, але не є достатньо ефективними для сучасного середовища кіберзагроз. Його ефективність можна оцінити як середню: базові процеси існують, але вони часто виконуються формально, без комплексного ризик-орієнтованого підходу.

Таблиця 2.2

Аналіз організаційного механізму забезпечення інформаційної безпеки у ДСБТ

Сильні сторони	Недоліки	Рекомендації
Наявність підрозділів/відповідальних осіб за ІБ.	Нестача кваліфікованих кадрів; обмежена роль керівництва у питаннях ІБ.	Посилити кадровий потенціал: створити окремий департамент кіберзахисту, забезпечити участь керівництва у прийнятті рішень.
Внутрішні накази та інструкції регламентують роботу з інформацією та доступами.	Більшість документів виконуються формально, за відсутності безперервного контролю.	Переглянути політики ІБ із переходом на ризик-орієнтований підхід; інтегрувати управління безперервністю (BCP/DRP).
Формалізована відповідальність у посадових інструкціях.	Відсутність ефективної системи KPI щодо дотримання вимог ІБ.	Ввести систему показників (KPI/SLI) для персоналу, що відповідає за ІБ.
Працівники ознайомлюються з вимогами ІБ при прийомі на роботу.	Слабка культура кібербезпеки.	Удосконалити програму постійного навчання: курси, симуляції фішингових атак, щорічні іспити.
Планові перевірки та контроль відповідності.	Аудит зосереджений на формальних документах, а не на практичній ефективності.	Впровадити внутрішній аудит ризиків та інцидентів, використати зовнішні незалежні перевірки.

Таким чином, організаційні механізми у ДСБТ можна оцінити як формально вибудувані з низьким рівнем зрілості. Їх модернізація потребує системності, кадрового підсилення та впровадження міжнародних практик.

Наступним кроком буде аналіз технічних засобів захисту з позиції оцінки ефективності управлінських механізмів ІБ у ДСБТ.

3.Технічні механізми – це інструменти та програмно-апаратні рішення, що підтримують управлінські політики та організаційні заходи в сфері інформаційної безпеки.

3.1. Криптографічний захист інформації (КЗІ): використовуються сертифіковані державою засоби шифрування (апаратні токени, ЕЦП/КЕП), які захищають документообіг, реєстри. Оцінка ефективності: забезпечує базову відповідність національним вимогам; не завжди інтегрований із сучасними європейськими чи міжнародними стандартами (AES-256, TLS 1.3, PKI).

3.2. Системи контролю доступу: використовуються засоби розмежування прав користувачів, паролі, облікові записи; частково реалізований контроль фізичного доступу до серверних. Оцінка ефективності: існує базова система аутентифікації; існує багатофакторна автентифікації (MFA) для всіх критичних систем.

3.3. Антивірусні системи та міжмережеві екрани (Firewall): встановлено стандартні антивірусні рішення; є міжмережеві екрани. Оцінка ефективності: захищає від поширених вірусів та несанкціонованого доступу; не покриває складні цілеспрямовані атаки (APT).

3.4. Моніторинг та реагування: наявні журнали подій, логування доступів; ведеться контроль використання КЗІ. Оцінка ефективності: базовий моніторинг працює; відсутня інтегрована DLP-система; реагування відбувається переважно постфактум, а не в реальному часі.

3.5. Резервування та відновлення даних: створюються резервні копії документів і баз даних. Оцінка ефективності: дозволяє мінімізувати втрати даних; є комплексної політики відновлення бізнес-процесів; резерви тестуються на працездатність. Загальна оцінка: технічні засоби захисту в ДСБТ забезпечують базовий рівень кіберзахисту, але не відповідають сучасному

рівню загроз і залишають критичні вразливості (відсутність сучасних SIEM, DLP, EDR, MFA).

Ефективність можна оцінити як середню (таблиця 2.3): виконуються мінімальні нормативні вимоги, але відсутня системна інтеграція сучасних технологій моніторингу й реагування. Відповідно, першочергові кроки – впровадження MFA для некритичних систем, удосконалення SIEM, EDR/DLP та оновлення криптографії.

Таблиця 2.3

Аналіз рівня забезпечення технічними засобами захисту інформації в системі інформаційної безпеки у ДСБТ

Сильні сторони	Недоліки	Рекомендації
Використання сертифікованих державних КЗІ.	Обмежена сумісність з міжнародними стандартами; недостатня адаптація до сучасних криптопротоколів.	Перехід на TLS 1.3, AES-256, впровадження PKI з урахуванням міжнародних вимог.
Наявність базових систем контролю доступу (паролі, журнали подій).	Відсутність MFA; слабкий захист привілейованих акаунтів.	Запровадити багатофакторну автентифікацію, PAM-рішення для адмін-акаунтів.
Антивірусні системи та Firewall забезпечують базовий захист.	Використовуються переважно сигнатурні методи; низька ефективність проти APT та zero-day атак.	Додати EDR/XDR з поведінковою аналітикою, оновити міжмережеві екрани до NGFW.
Ведеться логування та базовий моніторинг.	Відсутня централізована система (SIEM/DLP), немає кореляції подій.	Впровадити SOC/SIEM, інтегрувати DLP для запобігання витокам даних.
Виконуються резервні копії критичних даних, резерви тестуються.	Відсутня політика BCP/DRP	Створити план відновлення після інцидентів, тестувати резерви щоквартально.

Далі здійснимо аналіз управлінських процесів та моніторингу з позиції оцінки ефективності чинних управлінських механізмів забезпечення інформаційної безпеки в ДСБТ:

1. Планування та управління політиками. У ДСБТ діють внутрішні накази, положення та інструкції щодо поводження з інформацією. Політики ІБ здебільшого розроблені для виконання нормативних вимог. Оцінка ефективності: формалізований документообіг; політики не інтегровані у ризик-орієнтоване управління; слабкий зв’язок між стратегією відомства та цілями ІБ.

2. Управління ризиками: оцінка ризиків проводиться рідко; основний акцент робиться на усуненні виявлених порушень після перевірок. Оцінка ефективності: певні ризики враховуються (наприклад, при доступі до критичних систем); системного реєстру ризиків немає, відсутні методики вимірювання (KRI).

3. Моніторинг та контроль: використовується журналювання подій, контроль доступу, перевірки використання КЗІ; проводяться планові аудити відповідно до нормативів. Оцінка ефективності: є базовий рівень моніторингу (логування, контроль доступу); відсутня централізована система моніторингу (SIEM/SOC); інциденти розглядаються реактивно, а не в режимі реального часу.

4. Реагування на інциденти: при виявленні порушень складаються акти та видаються накази щодо усунення; інциденти фіксуються переважно у формі звітності після факту. Оцінка ефективності: наявний процес реагування; немає плану реагування на інциденти (IRP); відсутня координація з іншими держструктурами у режимі реального часу.

5. Аудит і вдосконалення: перевірки здійснюються відповідно до регламентів Держспецзв'язку; орієнтація переважно на дотримання вимог. Оцінка ефективності: забезпечується базова відповідність; аудити спрямовані на реальну оцінку ефективності, а не на розвиток системи.

Загальна оцінка: управлінські процеси та моніторинг у ДСБТ забезпечують базовий рівень функціонування, орієнтований на формальне дотримання законодавчих вимог; ризик-менеджмент та моніторинг слабкі, інциденти відслідковуються переважно постфактум.

Таким чином ефективність управлінських процесів та моніторингу з позиції забезпечення інформаційної безпеки у ДСБТ можна оцінити як середню: система працює, але не забезпечує проактивного захисту та своєчасного реагування. Отримані результати дозволяють зробити висновок, що правлінські процеси та моніторинг у ДСБТ забезпечують базовий контроль, але залишаються формальними та реактивними. Головні напрями вдосконалення: перехід до ризик-орієнтованого управління, централізований моніторинг (SIEM/SOC), формалізація IRP, регулярні незалежні аудити. Систематизація

переваг, недоліків і рекомендацій щодо управлінських процесів та моніторингу в ДСБТ наведено в додатку Б.

Для комплексного оцінювання поточного стану інформаційної безпеки у ДСБТ доцільним є застосування моделі зрілості управлінських процесів, що дозволяє визначити рівень формалізації, ефективності та інтегрованості механізмів кіберзахисту. Такий підхід дає змогу виявити прогалини, оцінити ступінь готовності організації до впровадження сучасних рішень та визначити пріоритетні напрями розвитку системи ІБ. У таблиці 2.4 наведено матрицю зрілості, яка відображає фактичний стан процесів та необхідні кроки для переходу на вищі рівні.

Таблиця 2.4

Матриця зрілості управлінських процесів та моніторингу інформаційної безпеки у ДСБТ

Рівень зрілості	Характеристика	Стан у ДСБТ	Що потрібно для переходу далі
1. Початковий (Initial)	Відсутні формалізовані процеси, реагування хаотичне.	Пройдено (система має певні регламенти).	×
2. Повторюваний (Repeatable)	Є базові інструкції та політики, виконання залежить від конкретних осіб.	Частково відповідає (наявні накази та журнали, але без системності).	Створити єдину систему політик ІБ, формалізувати процеси.
3. Визначений (Defined)	Процеси ІБ формалізовані, документовані, але не завжди ефективні.	Близький стан (політики є, але більше для «галочки»).	Впровадити ризик-орієнтоване управління, визначити KPI та KRI для ІБ.
4. Керований (Managed)	Є системна оцінка ризиків, централізований моніторинг (SIEM/SOC), план реагування (IRP).	Немає (моніторинг фрагментарний, IRP відсутній).	Запустити SIEM/SOC, розробити IRP, проводити симуляції інцидентів.
5. Оптимізований (Optimized)	Безпека інтегрована у всі управлінські процеси, діє проактивний моніторинг, постійне вдосконалення.	Не відповідає.	Впровадити автоматизацію (SOAR), інтегрувати управління ІБ у стратегічні цілі, проводити незалежні зовнішні аудити.

Отже, ДСБТ наразі знаходиться між рівнями 2 та 3 – процеси ІБ існують, але вони здебільшого формальні й не інтегровані у систему ризик-менеджменту. Щоб піднятися на рівень «Керований», першочергово необхідні:

централізований моніторинг (SIEM/SOC), план реагування на інциденти (IRP), регулярна оцінка ризиків та KPI. На рисунку 2.4. зображено матрицю зрілості управлінських процесів та моніторингу інформаційної безпеки у ДСБТ.

Рис. 2.4. Матриця зрілості управлінських процесів та моніторингу інформаційної безпеки у ДСБТ

Таким чином, ефективність чинних механізмів ДСБТ можна оцінити як середню: вони забезпечують базовий захист, але потребують модернізації для відповідності сучасним викликам. В додатку В наведено SWOT-аналіз ефективності управлінських механізмів інформаційної безпеки ДСБТ.

Отже, можна зробити висновок, що сильні сторони ДСБТ забезпечують базову відповідність вимогам законодавства та формують основу для розвитку, слабкі сторони свідчать про низьку проактивність: відсутність SIEM/SOC, IRP та системного ризик-менеджменту, можливості полягають у впровадженні сучасних моделей управління та інтеграції з державними і міжнародними стандартами; загрози підкреслюють актуальність термінової модернізації, оскільки рівень атак і ризиків зростає.

2.3. Визначення ризиків та загроз інформаційній безпеці в умовах цифровізації ДСБТ

У процесі цифрової трансформації діяльності Державної служби України з безпеки на транспорті значно зростає роль системного аналізу загроз та ризиків, що впливають на цілісність, доступність та конфіденційність інформаційних ресурсів. Розширення електронних сервісів, інтеграція міжвідомчих реєстрів, запровадження автоматизованих систем контролю та підвищення інтенсивності кіберзагроз у період воєнного стану формують нове, значно складніше середовище функціонування служби. За цих умов критично важливим є виявлення основних видів загроз – кібернетичних, технічних, організаційно-управлінських, правових та пов'язаних з людським фактором, які у своїй сукупності визначають загальний рівень вразливості інформаційної інфраструктури ДСБТ.

1. Загрози, пов’язані з кіберпростором становлять один із найбільш критичних факторів ризику для діяльності ДСБТ, оскільки спрямовані на порушення роботи державних реєстрів, цифрових сервісів та каналів міжвідомчої взаємодії. Основні види ризиків цієї групи загроз:

1.1 Кібератаки на інформаційні системи та державні реєстри. До найбільш поширених та небезпечних кіберзагроз належать: DDoS-атаки (Distributed Denial of Service), атаки типу SQL-injection та інші методи несанкціонованого доступу, спроби компрометації облікових даних користувачів.

1.2. Використання шкідливого програмного забезпечення. Шкідливе ПЗ є одним із найпоширеніших способів компрометації державних систем:

- Криптолокери (ransomware). У контексті ДСБТ це може блокувати: обробку порушень; роботу системи автоматизованих вагових комплексів WIM; доступ до ліцензійних процедур; зв’язок із територіальними управліннями.

- Spyware / Stealer-класи шкідливих програм.

- Trojan-класи програм. Містять «бекдори» для віддаленого доступу. Особливо небезпечні для систем, що працюють у мережі з декількома рівнями доступу.

1.3. Цілеспрямовані атаки на елементи критичної інформаційної інфраструктури. У структурі ДСБТ елементами критичної інформаційної інфраструктури є: сервери аналітичних даних; системи автоматизованих вагових комплексів (WIM); системи відеофіксації порушень; мережа обміну даними між центральним апаратом і територіальними органами; канали інтеграції з Мінцифрою, Держспецзв'язку та іншими органами. Цілеспрямовані атаки можуть мати такі наслідки: порушення функціонування процесів контролю на транспорті; спотворення або підміна даних про правопорушення; зниження достовірності даних державної статистики; виведення з ладу критичних систем у пікові періоди навантаження; збій у системах аналітики, що впливають на управлінські рішення.

1.4. Підсилення кіберзагроз умовами воєнного стану. Для державних органів, включно з ДСБТ, це проявляється у: збільшенні кількості спроб злому державних сервісів; підвищеній інтенсивності DDoS-атак; спробах отримати доступ до каналів міжвідомчої взаємодії; атаках на системи, пов'язані з транспортною інфраструктурою, що є критично важливою під час війни.

Загрози кіберпростору для ДСБТ мають багатовимірний характер і ускладнюються як розвитком цифрових сервісів, так і умовами воєнного стану.

2. Організаційні та управлінські ризики інформаційної безпеки в умовах цифровізації

Організаційні та управлінські ризики формують одну з найскладніших категорій загроз інформаційній безпеці, оскільки пов'язані не стільки з технічними чи зовнішніми факторами, скільки з внутрішніми процесами, регламентацією діяльності, кадровим потенціалом та системою управління інформаційними ресурсами. У структурі ДСБТ ці ризики набувають особливої значущості через розгалужену мережу територіальних органів, масштаб електронних сервісів, міжвідомчу взаємодію та постійне зростання обсягів оброблюваних даних.

2.1. Недостатня регламентація та стандартизація процесів інформаційної безпеки

Одним із ключових організаційних ризиків є відсутність або фрагментарність внутрішніх нормативних документів, що: регламентують порядок доступу до інформаційних систем; визначають ролі та зони відповідальності у сфері ІБ; встановлюють рівні класифікації даних та політики їхнього обробки; описують порядок реагування на кіберінциденти. В результаті виникає ризик нерівномірного застосування процедур різними структурними підрозділами та територіальними органами, що підвищує ймовірність інцидентів та ускладнює контроль.

2.2. Нерівномірний рівень цифрової компетентності персоналу

У ДСБТ працює великий штат співробітників із різним досвідом та кваліфікацією у сфері використання ІТ-систем. Основні ризики: помилки під час роботи з інформаційними ресурсами; необережне поводження з конфіденційною інформацією; схильність до фішингових атак; використання слабких паролів або повторне застосування credentials; порушення принципів розмежування доступу. Цей фактор є критичним, оскільки саме людська помилка генерує до 70% інцидентів у державному секторі.

2.3. Недостатність ресурсів для впровадження сучасних систем безпеки

Для системної кіберзахисту державні органи необхідні: SIEM-системи моніторингу подій безпеки; SOC-центри оперативного реагування; системи виявлення вторгнень (IDS/IPS); резервні майданчики та захищені канали зв'язку. У ряді випадків ДСБТ стикається з такими ризиками: обмежене фінансування на модернізацію ІТ-інфраструктури; недостатня кількість кваліфікованих фахівців із кіберзахисту; відсутність можливості забезпечити рівномірний рівень контролю у всіх територіальних органах; значна частка обладнання, що потребує оновлення.

2.4. Надмірна залежність від зовнішніх постачальників та підрядників

У цифровій інфраструктурі служби використовуються рішення зовнішніх розробників, які забезпечують: технічну підтримку; оновлення програмного забезпечення; доступ до системних модулів. Ризики: потенційна наявність слабких місць у сторонніх компонентах; можливість технічного впливу на критичні процеси (реєстри, фіксація порушень); залежність від графіка

обновлень, що може не відповідати рівню загроз; ризики компрометації під час передачі даних або адміністрування. Ця залежність ускладнюється тим, що частина сервісів інтегрована через міжвідомчі шлюзи (Мінцифра, Держспецзв'язку).

2.5. Ризики, пов'язані з територіальною розгалуженістю служби

ДСБТ має мережу територіальних органів у всіх областях України, що створює додаткові виклики: неоднаковий рівень технічного забезпечення; різний рівень дотримання політик безпеки; складність централізованого моніторингу кіберінцидентів; використання локальних ресурсів, які не завжди відповідають вимогам КСЗІ.

2.6. Недостатня культура управління ризиками

Основні прояви: нерегулярна ідентифікація та оцінка ризиків; відсутність централізованої бази кіберінцидентів; несистемність в управлінні доступами; недостатній контроль за виконанням вимог нормативних актів у сфері ІБ. Це ускладнює прийняття оперативних управлінських рішень та оцінку ймовірності повторних інцидентів.

3. Технічні ризики та загрози інформаційній безпеці ДСБТ – охоплюють спектр факторів, пов'язаних із станом, конфігурацією та рівнем захищеності інформаційно-комунікаційної інфраструктури ДСБТ.

3.1. Застарілість окремих компонентів ІТ-інфраструктури

До таких аспектів належать: серверне обладнання з обмеженими можливостями обробки та зберігання даних; операційні системи, що не підтримуються виробниками; системи управління базами даних старих версій; мережеве обладнання без підтримки актуальних протоколів захисту. Наслідками такого стану можуть бути: зниження продуктивності, збільшення часу обробки запитів, а також високий рівень вразливості до атак, спрямованих на експлуатацію відомих уразливостей.

3.2. Відсутність централізованого моніторингу та автоматизованих систем захисту

Цифрова інфраструктура державного органу потребує постійного моніторингу заходів безпеки. У ДСБТ ризики зростають через: часткову або

повну відсутність сучасних SIEM-систем, недосконаліть журналування подій, відсутність IDS/IPS-рішень на всіх критичних ділянках інфраструктури, відсутність єдиного центру реагування на інциденти (SOC). У таких умовах значно ускладнюється виявлення вторгнень, а реагування на інциденти часто здійснюється постфактумом, що збільшує масштаб можливих збитків.

3.3 Недостатність резервування та відмовостійкості

Складність інформаційних процесів ДСБТ вимагає створення резервних рішень із забезпеченням: дублювання серверних ресурсів; географічне резервування; резервного копіювання в реальному часі; безперервності доступу до критичних сервісів

Ризики виникають у випадках: відсутності Disaster Recovery Plan (DRP); нерегулярне тестування резервних копій; зберігання резервних даних у незахищених середовищах; відсутності альтернативних каналів зв'язку між територіальними органами та центральним апаратом. Наслідком може бути тривалий простий систем, повна або частична втрата даних.

3.4. Вразливості інтеграцій із зовнішніми регістрами та інформаційними системами.

ДСБТ інтегрована з низкою державних систем, зокрема: "Трембіта"; реєстрами Мінцифри; базами даних НПУ (у частині перевірки документів); реєстрами Держспецзв'язку; внутрішніми реєстрами Мінвідновлення.

Кожен такий канал інтеграції створює технічні ризики, пов'язані з: різним рівнем безпеки підключених систем; можливістю перехоплення або підміни даних під час обміну; недостатньою сегментацією мережевої інфраструктури; незахищеними API або застарілими інтерфейсами взаємодії. Це може призводити до порушення цілісності міжвідомчих даних або блокування критичних сервісів.

3.5. Недостатня сегментація та захист мережевої інфраструктури

У деяких випадках у територіальних органах спостерігається недостатня сегментація мереж, коли: внутрішні та службові системи існують в одній мережі; рівні доступу користувачів не розмежовані належним чином; мережа не поділена на зони безпеки (DMZ, внутрішня зона, критична зона). Це створює

умови для: горизонтального переміщення злодійника у разі проникнення; компрометації серверних ресурсів через робочі станції; масштабного поширення шкідливого ПЗ.

3.6. Наявність невиправлених вразливостей та проблем із оновленнями

Порушення політик оновлення може призводити до: накопичення відомих вразливостей; можливості віддаленого виконання коду; виконання атак на основі старих векторів, які давно закриті у сучасних версіях ПЗ.

Причинами є: відсутність централізованої політики обновлень; залежність від сторонніх підрядників; технічні обмеження застарілого обладнання; побоювання зупинки критичних сервісів.

3.7. Ризики, пов'язані з відеофіксацією та автоматизованими системами контролю.

ДСБТ використовує: відеокамери спостереження; автоматизовані вагові комплекси WIM; мобільні пристрої контролю. Технічні ризики: компрометація або підміна відеопотоку; втручання в канали передачі даних з пунктів контролю; фізичне пошкодження обладнання; підміна облікових записів операторів. Це може впливати на достовірність зафіксованих порушень та результати державного контролю.

4. Ризики, пов'язані з людським фактором. Незалежно від рівня технічної захисту, вразливість системи часто визначається поведінкою працівників, які мають доступ до інформаційних ресурсів

4.1. Ненавмисні порушення політик інформаційної безпеки

До найпоширеніших ризиків належать: неправильне поводження з конфіденційною інформацією; збереження службових документів на незахищених пристроях або в хмарних сервісах; передача робочих облікових даних третім особам; порушення встановлених правил класифікації та обробки інформації. Такі дії часто є наслідком недостатньої поінформованості, відсутності практичних навичок роботи у цифровій середовищі або недосконалої комунікації між підрозділами.

4.2. Низький рівень цифрової та кібергігієни працівників

Це один із ключових факторів вразливості державних органів. Серед найпоширеніших проявів: використання слабких паролів або їх повторне застосування; відсутність двофакторної аутентифікації; несвоєчасне оновлення програмного забезпечення на робочих станціях; нехтування базовими правилами кібербезпеки (відкриття підозрілих листів, перехід за шкідливими посиланнями тощо). Подібні дії значно підвищують ризик фішингових атак, зараження шкідливим ПЗ та компрометації облікових записів.

4.3. Схильність до соціальної інженерії

Зловмисники часто використовують методи соціальної інженерії, зокрема: фішингові електронні листи; підроблені повідомлення від керівництва чи партнерських організацій; дзвінки від "технічної підтримки"; підроблені сторінки авторизації.

Ризик зростає через: обмежену практичну підготовку співробітників недостатню обізнаність із сучасними методами маніпуляцій відсутність регулярних навчань із симуляціями атак. У державному секторі такі атаки особливо небезпечні, оскільки можуть призвести до витоку службових даних або доступу до критичних інформаційних систем.

4.4 Ризики навмисних порушень: інсайдерські загрози

Інсайдерські загрози (навмисні порушення працівників або колишніх співробітників) становитимуть особливо високий рівень ризику, оскільки: інсайдер має легітимний доступ до систем; знає вразливі місця організації; може діяти непомітно протягом тривалого часу. До таких порушень належать: умисне видалення або зміна даних; копіювання службової інформації; передання конфіденційних матеріалів третім особам; втручання в систему контролю або документообігу; навмисне порушення стабільності роботи IT-сервісів. Основні причини інсайдерських порушень: конфлікти інтересів, незадоволення умовами роботи, корупційні ризики чи зовнішній вплив.

4.5. Недостатня підготовка персоналу щодо роботи з IT-системами

Недостатній рівень підготовки персоналу може призводити до: некоректного внесення інформації до регістру; невірного налаштування техніки; порушення процедур доступу; зменшення ефективності використання

цифрових інструментів; помилок у роботі із системами контролю та відеофіксації. Це не лише створює ризики інформаційної безпеки, а й впливає на якість управлінських рішень.

4.6. Перевантаженість персоналу та стресові фактори

Умови воєнного стану, часта зміна пріоритетів, складна ситуація у сфері транспорту та велике навантаження на працівників призводять до: зниження концентрації уваги; збільшення кількості помилок; порушення процедур через поспіх; нехтування правилами безпеки в умовах стресу. Це є значним операційним ризиком, що потребує особливої уваги у контексті діяльності державних органів.

Ризики, пов'язані з людським фактором, є одними з найскладніших для управління, оскільки їх неможливо повністю усунути технічними засобами. Для їх мінімізації необхідні системні заходи: підвищення цифрової компетентності персоналу; регулярні тренінги з кібергігієни та протидії соціальної інженерії; формування культури інформаційної безпеки; контроль доступів та моніторинг поведінкових аномалій; створення середовища, що знижує ризики інсайдерських дій. Ефективне управління людським фактором є ключовою передумовою стійкості цифрових систем ДСБТ.

5. Правові та нормативні ризики інформаційної безпеки ДСБТ

Правові та нормативні ризики становлять важливу складову загальної системи загроз інформаційній безпеці, оскільки визначають рамкові умови функціонування інформаційних систем, порядок обробки даних, захист державної інформації та відповідальність посадових осіб.

5.1. Невизначеність чи прогалини в нормативно-правовому регулюванні.

Однією з основних загроз є те, що законодавство іноді не встигає за темпами цифровізації, що призводить до ризиків: відсутності єдиних вимог до кіберзахисту відомчих систем; нечітких процедур обміну даними між ДСБТ та зовнішніми органами (Мінцифра, НПУ, Мінвідновлення, Держспецзв'язку); правової невизначеності щодо використання нових цифрових технологій (візуальна аналітика, автоматизовані системи контролю, Big Data). Це може

створювати бар'єри для впровадження сучасних технічних рішень та ускладнювати узгодження політик безпеки.

5.2. Невідповідність внутрішніх документів сучасним вимогам.

Правові ризики виникають у разі, коли внутрішні положення, накази чи регламенти: застарілі чи не враховують нові інформаційні системи; не містять процедур реагування на кіберінциденти; не визначають порядок класифікації інформації та рівнів доступу; суперечити сучасному законодавству у сфері кіберзахисту. Такі невідповідності можуть призводити до того, що формально інформаційна політика існує, але не відповідає реальним умовам цифрового середовища.

5.3. Порушення вимог законодавства про захист персональних даних.

ДСБТ обробляє значні масиви персональних даних, зокрема: відомості про водіїв та перевізників; інформацію з автоматичної фіксації порушень; дані про ліцензійні заяви та результати перевірок. Ризики: некоректне зберігання або передавання таких даних; відсутність механізмів контролю за доступом до територіальних органів; порушення правил знеособлення даних; недостатня правова регламентація взаємодії з підрядниками. Наслідки можуть включати як втрату довіри громадськості, так і юридичну відповідальність.

5.4. Недотримання вимог законодавства у сфері криптографічної захисту.

Порушення вимог Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та нормативів Держспецзв'язку створює ризики: використання незатверджених криптографічних алгоритмів; неналежного керування ключами; відсутності сертифікованих засобів захисту; недотримання порядку атестації комплексної системи захисту інформації (КСЗІ). Порушення цих вимог може призвести до юридичної недійсності електронних даних або рішень, а також уразливості систем.

5.5 Невизначеність у правовому статусі автоматизованих систем контролю

Окремою групою ризиків є ті, що стосуються: систем автоматичної фіксації порушень на транспорті; вагових комплексів WIM; мобільних систем контролю.

Проблеми: неоднозначне трактування доказової сили технічних даних; відсутність правового механізму оскарження в разі технічних збоїв; неврегульованість процедур підтвердження цілісності даних. Це створює ризики як для правозастосування, так і для легітимності управлінських рішень.

5.6. Ризики, пов'язані з укладенням договорів та взаємодією з підрядниками.

У межах цифрової трансформації ДСБТ співпрацює з великою кількістю ІТ-компаній, що створює додаткові правові ризики: нечіткі умови відповідальності за кіберінциденти; відсутність у договорах вимог щодо КСЗІ, криптографічної захисту та обмеження доступу; ризик передачі стороннім особам прав адміністратора; неврегульованість обробки та зберігання службових даних. У разі правових прогалин виникають значні загрози для цілісності державних реєстрів.

5.7. Недостатня узгодженість між галузевим та загальнодержавним законодавством.

Цифровізація транспортної сфери розвивається швидше, ніж оновлюється: транспортне законодавство; нормативи державного контролю; правила надання адміністративних послуг. Це може призвести до правових колізій, коли одна частина законодавства дозволяє застосування цифрових сервісів, а інша не передбачає їх у правової моделі або не регулює їх використання.

Правові та нормативні ризики є системними та впливають на всі напрямки діяльності ДСБТ у сфері інформаційної безпеки. Їхнє своєчасне виявлення та управління є необхідною умовою: ефективної цифрової трансформації; легітимність використання електронних систем; належної захисту державної інформації; забезпечення довіри громадян та партнерських органів.

З метою систематизації результатів аналізу загроз було здійснено узагальнення ключових ризиків інформаційної безпеки, що формуються у процесі цифрової трансформації діяльності ДСБТ (таблиця 2.5).

Аналіз виявлених ризиків показує, що найбільш критичними для ДСБТ є загрози, пов'язані з кібератаками, шкідливим ПЗ та вразливістю критичної інфраструктури, оскільки вони безпосередньо впливають на безперервність

державного контролю та доступність адміністративних послуг. Значну групу формують організаційні та кадрові ризики, пов'язані з недостатньою регламентацією процесів інформаційної безпеки та низьким рівнем цифрової грамотності персоналу. Додатковий вплив мають технічні фактори – відсутність сучасних засобів моніторингу, слабкі інтеграційні канали та нестача резервування. Сукупність цих ризиків наголошує на необхідності комплексної модернізації системи ІБ ДСБТ, включно з оновленням інфраструктури, посиленням політик безпеки та підвищенням компетентностей персоналу.

Таблиця 2.5

Ключові ризики інформаційної безпеки ДСБТ в умовах цифрової трансформації

№	Ризик	Суть / чому є критичним
1	Кібератаки на державні регістри та цифрові сервіси (DDoS, SQL-injection)	Ураження реєстрів, перевантаження сервісів, підміна або видалення інформації безпосередньо впливають на роботу ДСБТ та доступ до адмінпослуг.
2	Використання шкідливого ПЗ, зокрема криптолокерів та троянів	Можливе повне блокування систем, шифрування даних та параліч вагових комплексів, відеофіксації та ліцензійних процедур.
3	Атаки на критичну інформаційну інфраструктуру (WIM, відеофіксація, аналітичні сервери)	Порушення державного контролю, втрата достовірності даних про правонарушення, зупинка роботи інфраструктури в пікові періоди.
4	Компрометація облікових даних персоналу (фішинг, соціальна інженерія)	Приводити до несанкціонованого доступу, зміни даних у регістрах та керуванні системами контролю.
5	Недостатність регламентації та політик ІБ у внутрішніх документах	Відсутність єдиних правил доступу та реагування на інциденти створює нерівномірний рівень безпеки та підвищує ризик інцидентів.
6	Низький рівень цифрової грамотності персоналу та помилки працівників	Саме людський фактор створює до 70% інцидентів у державних органах – від витоку даних до компрометації акаунтів.
7	Відсутність сучасних засобів моніторингу безпеки (SIEM, SOC, IDS/IPS)	Служба не має можливості оперативно виявляти та блокувати атаки, що збільшує їх масштаб та наслідки.
8	Залежність від зовнішніх IT-підрядників	Сторонні розробники мають доступ до критичних систем, а їх помилки, затримки з оновленнями чи вразливості можуть стати точкою атаки.
9	Вразливості мережевої інфраструктури та інтеграцій (API, «Трембіта», системи НПУ, Мінцифри)	Ризик перехоплення або підміни міжвідомчих даних, збій у роботі сервісів, велика залежність від безпеки суміжних систем.
10	Недостатність резервування, відмовостійкості та DRP	Відсутність резервних копій, дублювання серверів та плану відновлення може призвести до тривалих простоїв та втрати даних.

Для забезпечення об'єктивної оцінки рівня загроз було проведено кількісне ранжування ризиків за такими параметрами, як ймовірність настання, масштаб можливих наслідків та інтегральний рівень ризику. У таблиці 2.6 наведено результати оцінювання, що відображають ступінь опасности шкірного ризику та формують основу для подальшого планування заходів із захисту інформаційних ресурсів служби.

Таблиця 2.6

Матриця оцінювання ризиків інформаційної безпеки ДСБТ*

№ з/п	Ризик	Ймовір-ність (P)	Вплив (I)	Рівень ризику (R = P×I)	Оцінка критичності
1	Кібератаки на державні регістри та цифрові сервіси (DDoS, SQL-injection)	3	4	12	Критична
2	Використання шкідливого ПЗ, зокрема криптолокерів та троянів	2	4	8	Висока
3	Атаки на критичну інформаційну інфраструктуру (WIM, відеофіксація, аналітичні сервери)	2	4	8	Висока
4	Компрометація облікових даних персоналу (фішинг, соціальна інженерія)	3	3	9	Висока
5	Недостатність регламентації та політик ІБ у внутрішніх документах	2	2	4	Середня
6	Низький рівень цифрової грамотності персоналу та помилки працівників	3	2	6	Середня
7	Відсутність сучасних засобів моніторин-гу безпеки (SIEM, SOC, IDS/IPS)	2	4	8	Висока
8	Залежність від зовнішніх ІТ-підрядників	2	3	6	Середня
9	Вразливості мережевої інфраструктури та інтеграцій (API, «Трембіта», системи НПУ, Мінцифри)	2	3	6	Середня
10	Недостатність резервування, відмовостійкості та DRP	2	4	8	Висока

* Шкала оцінювання: P – Ймовірність: 1 - низька, 2 - середня, 3 - висока
I – Вплив: 1 - низька, 2 - середня, 3 - висока, 4 - критична
R – Критичність: 1-3 низька, 4-6 середня, 7-9 висока, ≥10 – критична

Для наочного відображення рівня небезпеки та взаємозв'язку між ймовірністю настання ризику та масштабом його впливу побудовано матрицю критичності ризиків інформаційної безпеки. Такий формат візуалізації дозволяє чітко визначити, які загрози становитиме найбільшу загрозу для стабільного функціонування інформаційних систем ДСБТ. Матриця (рисунок 2.5) також є основою для встановлення пріоритетів у плануванні заходів кіберзахисту.

Аналіз матриці показує, що найкритичнішим ризиком є загроза кібератак на державні регістри та цифрові сервіси (ризик №1), що поєднує високу ймовірність та максимальний рівень впливу. До групи високих ризиків також належать шкідливі ПЗ (№2), атаки на критичну інформаційну інфраструктуру (№3), компрометація облікових даних (№4) та недостатність резервування (№10). Ризики організаційного та технічного характеру, такі як уразливості інтеграцій (№9), залежність від підрядників (№8) чи недостатні політики ІБ (№5), мають середню критичність і потребують системного усунення.

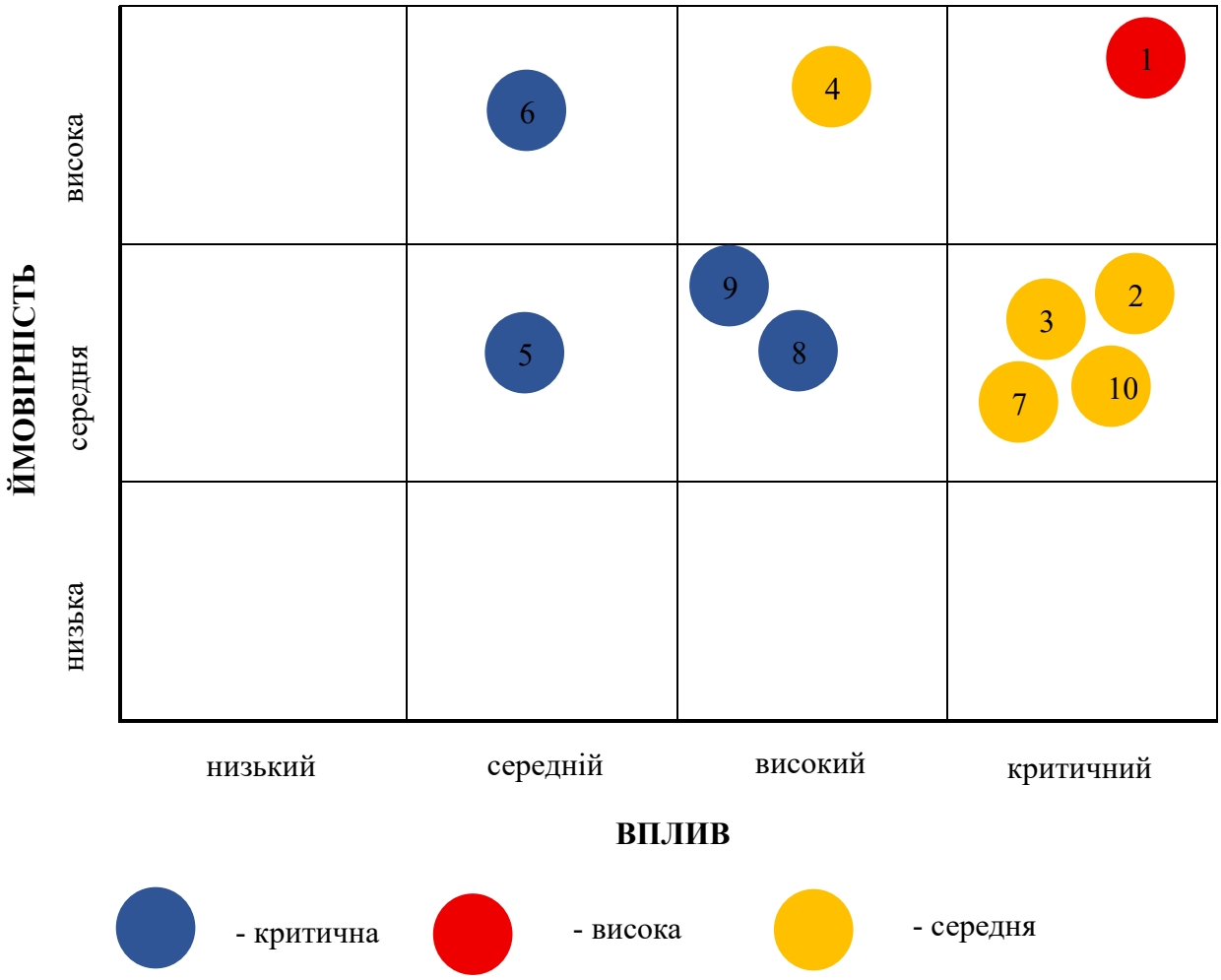

Рис. 2.5. Матриця критичності ризиків інформаційної безпеки ДСБТ в умовах цифрової трансформації

Така структура ризиків підтверджує необхідність комплексної модернізації ІТ-інфраструктури ДСБТ та підсилення управлінських механізмів кібербезпеки.

Для кількісної інтерпретації результатів оцінювання ризиків було здійснено їх ранжування за інтегральним показником критичності, що визначається як добуток ймовірності настання та масштабу впливу (рисунок 2.6). Середні значення інтегрального показника демонструють організаційні та технічні ризики, пов'язані з політиками безпеки, цифровою грамотністю персоналу, інтеграціями та залежністю від підрядників.

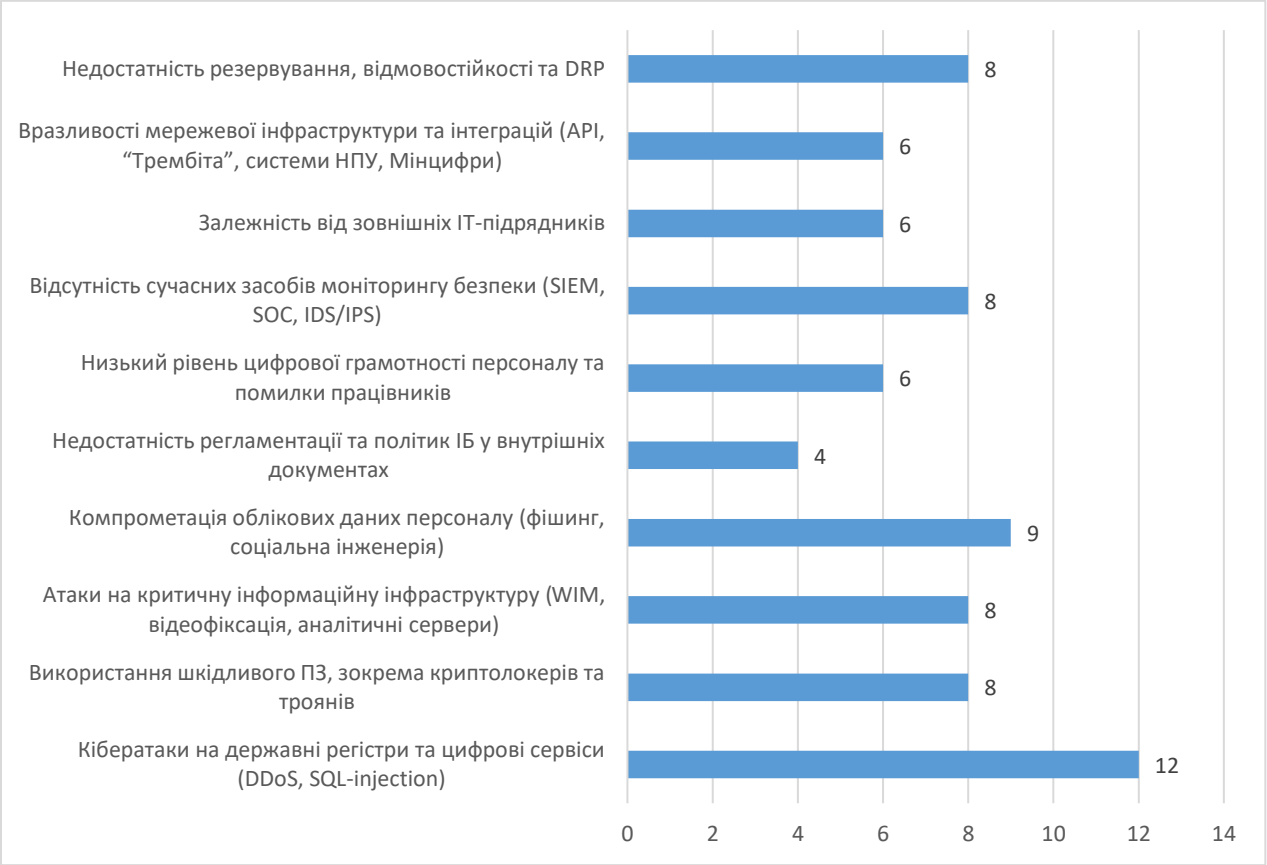

Рис. 2.6. Ранжування ризиків інформаційної безпеки ДСБТ за рівнем критичності

Такий розподіл підкреслює важливість одночасного посилення як технічних заходів кіберзахисту, так і управлінських підходів до забезпечення інформаційної безпеки.

Висновки до розділу 2:

Проведений аналіз у розділі 2 дозволяє комплексно оцінити стан системи інформаційної безпеки ДСБТ та визначити ключові проблеми, що стримують її розвиток в умовах цифрової трансформації. Дослідження організаційної структури та нормативно-правового забезпечення засвідчило, що в службі вже сформовано основні елементи моделі ІБ – спеціалізовані підрозділи, нормативні документи, визначені процедури взаємодії та канали координації з національними центрами кіберзахисту. Водночас їхня узгодженість і структурна зрілість залишаються недостатніми, що зумовлює фрагментованість політик, дублювання функцій та нерівномірний рівень захищеності в різних підрозділах.

Оцінка ефективності чинних управлінських механізмів показала, що цифровізація ключових процесів та впровадження електронних реєстрів позитивно вплинули на прозорість і контроль доступу до даних. Разом із тим існує низка системних обмежень: недостатній рівень інтеграції інформаційних систем, різна якість підготовки персоналу, неврегульованість окремих процесів реагування на інциденти, обмежені ресурси підрозділів ІБ. Навіть за наявності позитивної динаміки, ефективність управлінських інструментів залишається нерівномірною, що підкреслює потребу переходу до централізованої моделі управління інформаційною безпекою.

Аналіз ризиків та загроз показав, що цифровізація, хоч і розширює функціональні можливості служби, водночас підвищує її вразливість до кіберзагроз. Серед найбільш критичних ризиків – кібератаки, людський фактор, неузгодженість процедур, збої в інтеграції систем, вразливості каналів обміну даними та збільшення навантаження на інфраструктуру. Сукупність цих факторів свідчить, що система ІБ ДСБТ перебуває у фазі розвитку та потребує зміцнення як технічної, так і управлінської складових.

Отже, нинішня система інформаційної безпеки має потенціал, але її ефективність обмежена фрагментарністю, різним рівнем процесної зрілості підрозділів і недостатньою інтегрованістю механізмів захисту.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДСБТ

3.1 Стратегічні напрямки удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки ДСБТ

Аналіз діяльності ДСБТ показує, що існуюча модель забезпечення ІБ має низку обмежень, зображених на рисунку 3.1:

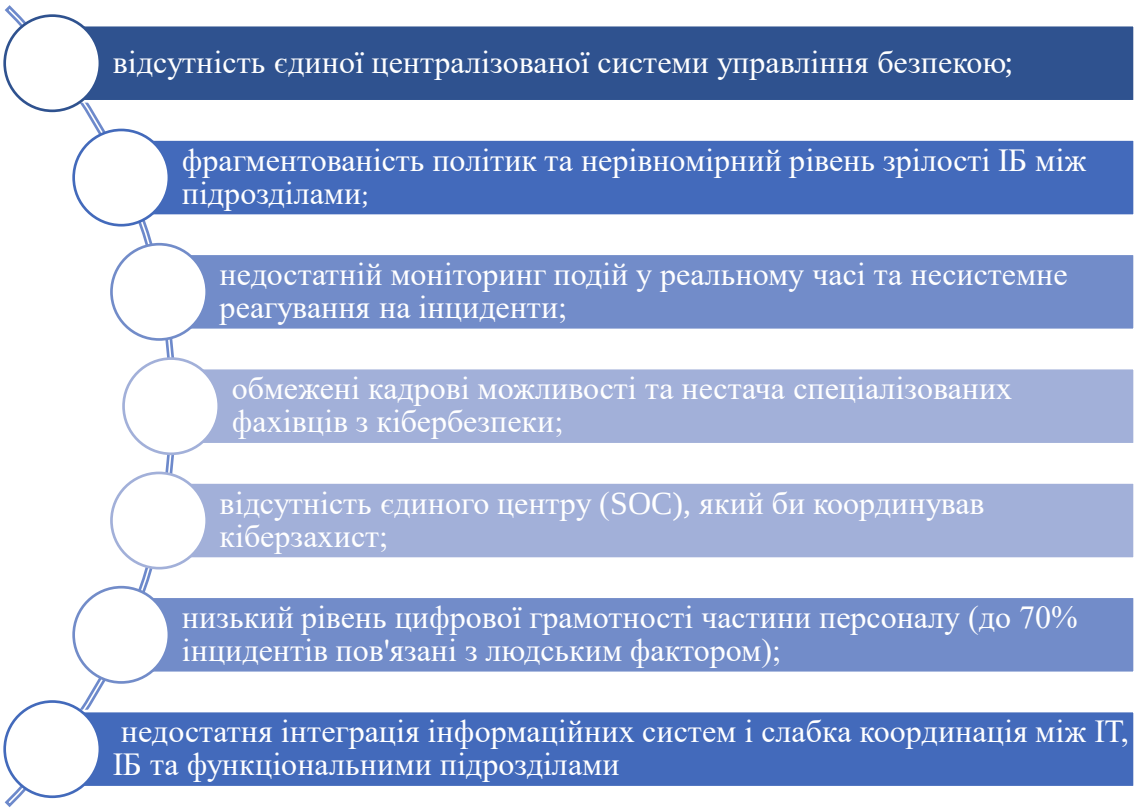

Рис. 3.1. Основні обмеження чинної моделі забезпечення інформаційної безпеки ДСБТ

Ці фактори створюють передумови для ризиків, сформульованих у розділі 2, і вимагають побудови цілісної системи, здатної забезпечити безперервний моніторинг, реагування, стандартизоване управління та захищеність інформаційних ресурсів.

Для підвищення кіберстійкості ДСБТ доцільно впровадити такі ключові організаційно-управлінські заходи:

1. Формування інтегрованої системи управління інформаційною безпекою (ISMS): розроблення та впровадження політик, процедур та стандартів відповідно до ISO/IEC 27001; визначення відповідальності за ІБ на кожному рівні управління; впровадження циклу PDCA (Plan-Do-Check-Act) у сфері ІБ.

2. Створення Центру моніторингу та реагування на інциденти (SOC): впровадження SIEM-платформи для централізованого збирання логів; створення цілодобової функції реагування (Tier 1-3); інтеграція з CERT-UA та Держспецзв'язку.

3. Посилення ролі ризик-менеджменту: впровадження єдиної методики оцінювання ризиків; регулярне оновлення карти ризиків ІБ; визначення власників ризиків та контрольних заходів.

4. Розвиток кадрового потенціалу: формування внутрішньої команди ІБ; регулярні тренінги, симуляційні навчання (phishing simulation, table-top exercises); навчання персоналу засадам кібергігієни.

5. Удосконалення управління доступом та наданням прав: впровадження MFA на всі критичні системи; регулярний аудит облікових записів; централізація систем керування ідентичностями (IAM).

6. Підвищення стійкості інформаційної інфраструктури: впровадження DRP-плану та резервування критичних сервісів; щорічне тестування безперервності (BCP/DRP tests); аудит інтеграційних каналів та API.

Ці заходи повинні бути реалізовані поетапно відповідно до дорожньої карти розвитку системи ІБ (рис. 3.2).

Реалізація запропонованих заходів дозволить: сформувати цілісну систему управління інформаційною безпекою; знизити рівень критичних ризиків ІБ (кібератаки, компрометація даних, збої інтеграцій); підвищити рівень прозорості, керованості та передбачуваності процесів безпеки; забезпечити відповідність вимогам міжнародних стандартів та державним політикам у сфері захисту інформації; підвищити кіберстійкість ДСБТ та готовність до інцидентів; забезпечити безпечну цифровізацію послуг та зменшити кількість інцидентів, спричинених людським фактором.

Рис. 3.2. Дорожня карта розвитку системи інформаційної безпеки ДСБТ (0-5 років)

Таким чином, стратегічні напрямки удосконалення ІБ у ДСБТ формують підґрунтя для переходу до зрілої, ефективної та стійкої моделі управління безпекою, здатної підтримувати масштабовану цифрову трансформацію служби.

3.2 Використання сучасних технологій кіберзахисту та удосконалення операційних процесів забезпечення інформаційної безпеки в ДСБТ

Для забезпечення послідовності, обґрунтованого розподілу ресурсів та узгодженості з дорожньою картою розвитку ІБ, доцільно визначити

пріоритетність впровадження технічних рішень. Матриця пріоритетності (таблиця 3.1) дозволяє систематизувати рекомендації за рівнями терміновості та стратегічної важливості та формує основу для планування бюджету, технічних завдань та управлінських рішень у сфері ІБ.

Таблиця 3.1

Матриця пріоритетності модернізації технічних засобів захисту ДСБТ

Пріоритет	Напрям	Що потрібно зробити	Термін реалізації
Високий (негайно)	Контроль доступу	Впровадити MFA для некритичних систем; PAM для адмін-акаунтів.	0-6 місяців
	Моніторинг	Запуск пілотної SIEM (збір логів з критичних вузлів).	0-12 місяців
	Антивірус/EDR	Оновити антивірусні рішення, додати EDR/XDR для захисту від APT.	0-12 місяців
Середній (середньо-строково)	Криптографія	Перехід на сучасні стандарти (AES-256, TLS 1.3, PKI).	1-2 роки
	DLP	Впровадити систему запобігання витокам даних.	1-2 роки
	Резервування	Створити політику BCP/DRP, тестувати резервні копії.	1-2 роки
Низький (довго-строково)	Архітектура	Перехід на модель Zero Trust, сегментація мереж.	3-5 років
	Автоматизація	Впровадження SOAR для автоматизованого реагування.	3-5 років
	Сертифікація	Сертифікація системи ІБ за ISO/IEC 27001.	3–5 років

Аналіз наведеної матриці демонструє необхідність концентрації ресурсів у короткостроковій перспективі на засобах контролю доступу, моніторингу подій безпеки та виявлення загроз, оскільки саме ці компоненти забезпечують мінімізацію найбільш критичних ризиків (кібератаки, компрометація даних, несанкціонований доступ). Середньострокові заходи спрямовані переважно на підвищення рівня стійкості систем та запобігання витокам інформації, що відповідає переходу до більш зрілої, керованої моделі ІБ. Довгострокові напрями – зміна архітектури, автоматизація реагування та сертифікація – орієнтовані на стратегічну трансформацію та досягнення рівня «Оптимізований» відповідно до міжнародних стандартів та сучасних практик кіберзахисту.

Ефективне функціонування системи інформаційної безпеки ДСБТ неможливе лише за рахунок організаційних реформ чи технічної модернізації. Необхідною умовою формування цілісної, керованої та стійкої моделі є удосконалення операційних процесів, які забезпечують реальне щоденне функціонування механізмів кіберзахисту.

Одним із ключових елементів операційної моделі є формування процесу управління інцидентами. Створення плану реагування (IRP), визначення ролей та процедур ескалації, а також документування та проведення постінцидентного аналізу забезпечують не лише швидке відновлення роботи критичних сервісів, а й накопичення знань для попередження повторних інцидентів. Враховуючи пріоритет запуску SIEM та формування майбутнього SOC, визначеного у технічній матриці модернізації, стандартизований процес інцидент-менеджменту дозволить забезпечити координацію між технічними та управлінськими підрозділами, а також взаємодію з CERT-UA та Держспецзв'язку.

Важливим напрямом є запровадження системного управління вразливостями, що включає регулярні сканування, аналіз результатів за методологією CVSS, пріоритизацію виправлень та контроль виконання патч-менеджменту. У розділі 2 було визначено наявність низки технічних та організаційних вразливостей, що підвищують ризик компрометації даних. Запровадження централізованого процесу управління вразливостями дозволить зменшити площину атаки, забезпечити прозорість відповідальності та інтегрувати цю діяльність із модернізаційними пріоритетами (зокрема EDR/XDR, DLP і криптографічними рішеннями).

Окремої уваги потребує вдосконалення контролю доступу та управління життєвим циклом облікових записів. Наявність у ДСБТ великої кількості інтегрованих систем і різнорівневих користувацьких ролей зумовлює необхідність чітких процедур onboarding/offboarding персоналу, періодичного перегляду привілеїв, контролю службових облікових записів і журналювання адміністративних дій. Поєднання цих практик із технічними рішеннями MFA,

IAM та PAM, створює підґрунтя для здобуття контролю над критичними ресурсами та зниження ризику несанкціонованого доступу.

Операційна підтримка технічної інфраструктури кіберзахисту охоплює регулярний моніторинг логів, тестування резервних копій, контроль працездатності каналів обміну даними та перевірку відповідності конфігурацій політикам безпеки. Ураховуючи визначені у розділі 2 проблеми із застарілими механізмами захисту та недостатньою деталізацією аудиту, формалізація цих процедур дозволить підвищити рівень прозорості та передбачуваності роботи систем ІБ.

Значущою складовою операційних процесів є розвиток культури кібергігієни персоналу. Проведення регулярних тренінгів, симуляцій фішингових атак, інформаційних кампаній, розробка чеклістів безпечної поведінки та періодичні оцінювання знань персоналу формують відповідальне ставлення до інформаційних ресурсів і зменшують ризик інцидентів, спричинених людським фактором. У розділі 2 саме людський фактор визначено як один із ключових ризиків, що підтверджує необхідність системної освітньої та комунікаційної роботи.

Для формування сталої культури інформаційної безпеки у ДСБТ важливо впровадити структуровану систему навчання персоналу, яка охоплює різні категорії співробітників та відповідає рівню їхніх функціональних обов’язків. Визначені тренінгові програми дозволяють забезпечити як базову цифрову грамотність, так і поглиблену компетентність для ІТ та керівного складу. У таблиці представлено перелік навчальних курсів, рекомендованих до впровадження, із зазначенням тривалості, аудиторії, періодичності та ключових показників ефективності.

Підвищення рівня кібергігієни персоналу є ключовим елементом зміцнення операційної безпеки ДСБТ та зниження ризиків, пов'язаних із людським фактором. В таблиці 3.2 представлено систематизовані напрямки та заходи, спрямовані на формування зрілої культури інформаційної безпеки. Запропоновані заходи дозволяють сформувати цілісну систему розвитку цифрової грамотності та кіберсвідомості персоналу ДСБТ.

Таблиця 3.2

Рекомендовані заходи щодо розвитку культури кібергігієни персоналу ДСБТ

№	Напрям	Опис заходів	Періодичність / Формат	Ціль / KPI
1	Регулярні тренінги (обов'язкова програма)	2 базових модулі (фішинг, паролі, файли) 1 спецмодуль для керівників/адміністраторів	1 раз на 6 місяців Формат: відеокурси, тестування, практичні модулі	100% охоплення персоналу Наразі 60% (437 осіб) → необхідно охопити +291 особу
2	Симуляції фішингових атак	Виявлення ризику, аналіз динаміки, зниження кількості переходів за шкідливими посиланнями	Щомісяця	KPI: поточний – 15% переходів через 6 міс – ≤10% через 12 міс – ≤5%
3	Інформаційні кампанії	щотижневі короткі матеріали, щоквартальні поглиблені рекомендації, кібер-дайджест email, плакати у регіонах, внутрішній портал «Кібербезпека ДСБТ»	Щотижня / щокварталу	Підвищення обізнаності; стабільне зниження людського фактору
4	Чеклісти безпечної поведінки	Для всіх співробітників: перевірка вкладень, правила створення паролів, використання КЕП, дії при підозрілих листах. Для ІТ/ІБ: журналювання, оновлення систем,контроль привілеїв	Постійно (оновлення раз на 6 міс)	100% доступності чеклістів; зниження інцидентів, пов'язаних із помилками користувачів
5	Оцінювання знань персоналу	Тестування, визначення груп ризику, коригування навчальних програм	2 рази на рік	KPI: ≥ 85% результатів тестів; формування планів корекції для груп ризику
6	Рольова модель (Role-based Cyber Training)	Різні програми для: інспекторів, регіональних підрозділів, аналітиків, адміністраторів, керівників	1 раз на рік для кожної ролі	Створення 100% ролевих програм; охоплення всіх груп персоналу

Реалізація цих рекомендацій сприятиме підвищенню загального рівня кіберстійкості та операційної надійності установи. В додатку Г наведено перелік тренінгових програм з кібергігієни та інформаційної безпеки для персоналу в ДСБТ

Запропоновані тренінги охоплюють усі ключові напрями розвитку компетентностей з інформаційної безпеки та забезпечують системний підхід до

зниження інцидентів, пов’язаних із людським фактором. Використання чітких KPI дозволяє оцінювати ефективність кожного навчального заходу та коригувати програму відповідно до потреб ДСБТ. Упровадження цієї навчальної матриці сприятиме формуванню зрілої моделі кіберкультури та підвищенню загального рівня кіберстійкості органу.

Проведемо аналітичні розрахунки:

- Розрахунок обсягу навчання: 728 співробітників × 2 базових модулі = 1 456 модуль-проходжень за півроку; додатково 1 модуль для 182 керівників/адміністраторів (умовно 25% штату) = 182 модулі; сумарний навчальний обсяг: 1 638 модуль-проходжень / 6 місяців

- Розрахунок ресурсів для симуляцій фішингу: кількість співробітників: 728, симуляції: 12 разів на рік, бсяг e-mail розсилок: 728 × 12 = 8 736 тестових листів щорічно, очікувана кількість переходів (якщо не впроваджувати навчання): 15% × 8 736 ≈ 1 310 ризикових взаємодій

Ціль після навчання: ≤5%: 5% × 8 736 ≈ 437 переходів

Зниження ризику: на 873 випадки (- 66%)

- Економічний ефект (спрощений розрахунок):

Середня вартість інциденту через людський фактор у держорганах України ≈ 2000 грн (втрати часу + відновлення + техпідтримка).

Поточний рівень ризику: ≈1 310 інцидентів × 2000 грн = 2 620 000 грн

Після впровадження програми (ціль ≤5%): 437 інцидентів × 2000 грн = 874 000 грн.

- Економія для ДСБТ: ≈ 1 746 000 грн на рік

Проведений розрахунок показує, що щорічно співробітники ДСБТ повинні пройти 1 638 модуль-проходжень з кібергігієни, а загальна кількість фішингових симуляцій становитиме близько 8 736 тестових листів. Очікуване зниження рівня переходів за шкідливими посиланнями з 15% до 5% дозволить скоротити ризики, пов’язані з людським фактором, на 66% та зменшити потенційні збитки орієнтовно на 1,7 млн грн щорічно. Для оцінки ефективності заходів із підвищення рівня цифрової грамотності та кібергігієни персоналу ДСБТ доцільно визначити ключові показники результативності. У таблиці

наведено систему KPI, що дозволяють вимірювати динаміку прогресу протягом найближчих шести та дванадцяти місяців. Такі індикатори забезпечують можливість об’єктивної оцінки впливу людського фактору та коригування навчальних і організаційних заходів.

Таблиця 3.3

Цільові показники розвитку кібергігієни та зниження впливу людського фактору на ДСБТ

Показник	Поточний рівень	Ціль 6 міс	Ціль 12 міс
Охоплення тренінгами, %	60	80	100
Фішинг-click rate, %	15	≤10	≤5
Підготовленість керівників, %	30	70	100
Наявність ролевих програм, %	немає	50	100
Кількість інцидентів через людський фактор	~1 300	≤700	≤450

Досягнення цільових значень протягом року забезпечить підвищення рівня кіберстійкості ДСБТ та формування сталої культури інформаційної безпеки серед співробітників.

Загалом удосконалення операційних процесів забезпечує перехід від фрагментарної моделі роботи до цілісної операційної екосистеми інформаційної безпеки, що підтримує технічні, управлінські та нормативні зміни. Реалізація цих заходів дозволить підвищити рівень кіберстійкості ДСБТ, забезпечити відповідність новим технічним рішенням, визначеним вище, та створити основу для інтегрованої системи управління безпекою відповідно до стратегічних напрямів, визначених у підрозділі 3.1.

3.3 Запровадження системи моніторингу та оцінки ефективності заходів з інформаційної безпеки

Реагування на інциденти включає у собі сукупність організаційних, технічних та управлінських заходів, спрямованих на виявлення, локалізацію, усунення наслідків та запобігання повторним подіям. У 2024 році робота служби демонструє часткову сформованість процесів реагування. Зокрема, впровадження Єдиного комплексу інформаційних систем, активний розвиток

цифрових реєстрів та навчання персоналу сприяють покращенню здатності виявляти загрози та мінімізувати їх вплив. Однак необхідно зазначити, що відсутність повноцінної інфраструктури на кшталт SOC, SIEM або централізованих IDS/IPS-рішень обмежує можливості швидкої ідентифікації інцидентів та масштабного моніторингу подій безпеки.

Загалом ефективність реагування ДСБТ на інциденти можна охарактеризувати як помірну, оскільки сформовано базові механізми, але відсутні необхідні технологічні платформи та регламентовані процедури, що дозволили б створити повноцінну систему швидкого та проактивного реагування. Для підвищення рівня необхідні: впровадження централізованого SOC, розвиток систем моніторингу, стандартизація процесів реагування та регулярне тестування готовності персоналу.

Для ДСБТ критично важливою є єдина інтегрована система логування та обробки подій безпеки, що охоплює як центральний апарат, так і всі територіальні органи. Оцінювання здійснюється за допомогою ключових показників ефективності (KPI) та показників рівня сервісу (SLA) . Основними метриками, що використовуються для оцінки роботи системи ІБ, є наступні:

1. MTTD – середній час виявлення інциденту (Mean Time To Detect) – середнє значення, яке показує, наскільки оперативно організація здатна помічати інциденти

$$\text{MTTD} = \frac{\sum_{i=1}^{N_{\text{det}}} T_{\text{detect},i}}{N_{\text{det}}} \tag{3.1}$$

де: $T_{\text{detect},i}$ – час виявлення i -го інциденту (у хвилинах/годинах), тобто проміжок від моменту виникнення інциденту до його фіксації службою; $\sum T_{\text{detect},i}$– сумарний час виявлення всіх інцидентів за аналізований період; N_{det}– кількість інцидентів, які були виявлені за період.

2. MTTR – середній час усунення інциденту (Mean Time To Recover/Remediate) – середній час відновлення, що відображає оперативність реагування

$$\text{MTTR} = \frac{\sum_{i=1}^{N_{\text{res}}} T_{\text{remediate},i}}{N_{\text{res}}} \tag{3.2}$$

де: $T_{\text{remediate},i}$ – час, витрачена на повне усунення i -го інциденту (від моменту виявлення до повного відновлення); $\sum T_{\text{remediate},i}$ – сумарний час, витрачений на усунення всіх інцидентів; N_{res} – кількість інцидентів, для яких завершено роботи з відновлення.

3. Коефіцієнт виявлення інцидентів (Detection Rate) – частка інцидентів, які служба змогла виявити

$$\text{Detection Rate} = \frac{N_{\text{det}}}{N_{\text{attempt}}} \times 100\% \tag{3.3}$$

де: N_{det} – кількість інцидентів, які фактично були виявлені; N_{attempt}- загальна кількість спроб атак, зафіксованих зовнішніми чи внутрішніми системами моніторингу (або оціночною моделлю).

4. Коефіцієнт локалізації інцидентів (Containment Rate) – показує, як ефективно служба стримує інциденти на ранніх етапах

$$\text{Containment Rate} = \frac{N_{\text{contained}}}{N_{\text{det}}} \times 100\% \tag{3.4}$$

де: $N_{\text{contained}}$– кількість інцидентів, які вдалося локалізувати до того, як вони розповсюдилися; N_{det} – кількість виявлених інцидентів

5. Виконання SLA щодо обробки інцидентів (SLA compliance) – відсоток виконання встановлених часових норм

$$\text{SLA\_compliance} = \frac{N_{\text{SLA}}}{N_{\text{det}}} \times 100\% \tag{3.5}$$

де: N_{SLA} – кількість інцидентів, які були закриті в межах ухвалених нормативів (SLA – Service Level Agreement); N_{det} – кількість виявлених інцидентів.

6. Рівень відновлення після інцидентів (Recovery Rate) – показує результативність завершення процесу реагування

$$\text{Recovery Rate} = \frac{N_{\text{recovered}}}{N_{\text{det}}} \times 100\% \tag{3.6}$$

де: $N_{\text{recovered}}$ – кількість інцидентів, після яких повністю відновлено систему/дані; N_{det} – загальна кількість виявлених інцидентів.

7. Очікувані збитки від інцидентів (Expected Loss / Risk Exposure) – інтегральний показник ризикового навантаження на організацію

$$\text{Expected Loss} = \sum_{i=1}^{n} p_i \times L_i \tag{3.7}$$

де: p_i – ймовірність настання i -го ризику за період; L_i – очікуваний розмір збитків у разі реалізації цього ризику (у грошовому еквіваленті).

8. Економічний ефект від впровадження засобів безпеки (ROSI) – показує економічну доцільність інвестицій у кіберзахист

$$\text{ROSI} = \frac{\text{Expected Loss}_{\text{before}} - \text{Expected Loss}_{\text{after}} - \text{Cost}_{\text{security}}}{\text{Cost}_{\text{security}}} \quad (3.8)$$

де: Expected Loss_before – очікувані збитки до впровадження заходів безпеки, Expected Loss_after – очікувані збитки після впровадження заходів, Cost_security – витрати на впровадження засобів безпеки.

Регулярний аналіз динаміки цих показників дозволяє оцінити, як саме впроваджені заходи (оновлення обладнання, навчання, політики, системи контролю) впливають на реальний рівень захищеності.

Вхідні дані, що використовуються у розрахунках:

Кількість виявлених інцидентів за період:$N_{\text{det}} = 120$.

Сумарний час виявлення всіх інцидентів:$\sum T_{\text{detect}} = 3600$хв.

Кількість усунутих інцидентів:$N_{\text{res}} = 110$.

Сумарний час на усунення всіх усунених інцидентів:$\sum T_{\text{remediate}} = 7200$хв.

Кількість інцидентів локалізованих до розповсюдження:$N_{\text{contained}} = 95$.

Кількість інцидентів, закритих у межах SLA:$N_{\text{SLA}} = 80$.

Для коефіцієнта виявлення допустимо оцінку загальних спроб атак:$N_{\text{attempt}} = 150$.

Для Expected Loss $= 360\,000$ грн.

Для ROSI наведемо 2 сценарії з різними припущеннями витрат на захист.

Система моніторингу інформаційної безпеки повинна функціонувати як неперервний процес, спрямований на: своєчасне виявлення аномалій, потенційних вторгнень та порушень політик безпеки; оцінку рівня дотримання норм і вимог КСЗІ в центральному апараті та територіальних органах; формування управлінської аналітики для прийняття рішень щодо модернізації ІТ-інфраструктури; забезпечення централізованого збору інцидентів та подій безпеки.

Таблиця 3.4

Показники ефективності реагування на інциденти інформаційної безпеки ДСБТ

Показник	Розрахунок (формула)	Норматив / Цільовий показник	Коментар
MTTD	$\frac{3600}{120} = 30$ хв	< 60 хв (оптимально - < 30 хв)	Показник відповідає кращим практикам; свідчити про прийнятну оперативність виявлення.
MTTR	$\frac{7200}{110} = 65{,}45$ хв	< 240 хв (оптимально < 120 хв)	Час усунення інцидентів є досить швидким для державного сектору.
Detection Rate	$\frac{120}{150} \times 100\% = 80\ \%$	> 85%	Показник високий, однак є потенціал підвищити до рівня 85–90 %.
Containment Rate	$\frac{95}{120} \times 100\% = 79{,}17\ \%$	> 80%	Значення прикордонне; рекомендується покращення через автоматизацію реагування.
Виконання SLA щодо інцидентів	$\frac{80}{120} \times 100\% = 66{,}67\ \%$	> 90%	Показник недостатній; свідчити про низький рівень процесної зрілості реагування.
Incident Volume (обсяг інцидентів)	120	Немає нормативу (динаміку порівнюють за роками)	Потребує аналізу тенденцій; може свідчити про загальну загрозливу ситуацію.
Recovery Rate	$\frac{110}{120} \times 100\% = 91{,}67\ \%$	> 90%	Хороший показник; система переважно повертається до штатної роботи.
Expected Loss	$\sum p_i L_i = 360000$	Зменшення на ≥30 % після впровадження заходів	Середня величина ризикового навантаження. Може бути базою для ROSI.
ROSI (оптимістичний сценарій)	$(360000 - 180000 - 150000)/15000 = +20\ \%$	> 0 % (окупність інвестицій)	Інвестиція в кіберзахист економічно доцільна.
ROSI (песимістичний сценарій)	$(360000 - 250000 - 200000)/20000 = -45\%$	> 0%	У разі високої вартості інвестиції проект стає економічно ризикований

Запровадження ефективної системи M&E (Monitoring and Evaluation) передбачає використання таких інструментів:

1. SIEM-система (Security Information and Event Management) забезпечує збір логів із серверів, мережевого обладнання, прикладних систем та платформ контролю, а також здійснює кореляцію подій для виявлення атак.
2. IDS/IPS-рішення (Intrusion Detection/Prevention Systems) – рацюють як перший рубіж виявлення вторгнень, дозволяють блокувати нетипові поведінкові паттерни та небезпечний мережевий трафік.
3. Система централізованого управління доступами (IAM/PAM) Дає змогу відстежувати всі дії користувачів, адміністративні зміни та спроби несанкціонованого доступу.
4. Журналювання подій у критичних системах (WIM, відеофіксація, регістри) – дозволяє формувати повний ланцюг подій (audit trail), необхідний для аналізу інцидентів.
5. SOC (Security Operations Center) у форматі власного чи віддаленого центру реагування – підвищує швидкість обробки інцидентів та забезпечує цілодобовий моніторинг.

Система M&E повинна бути організована на трьох рівнях:

Операційний рівень – первинний збір даних, автоматизований моніторинг, сигналізація про інциденти.

Аналітичний рівень – аналіз тенденцій, формування звітів, кореляція подій.

Стратегічний рівень – оцінка ефективності політик, затвердження річних планів захисту, перегляд ризикової моделі.

Ключова роль у цьому процесі належить Управлінню інформаційної безпеки, яке виконує функції координації, аудиту та підготовки аналітичних звітів.

Система моніторингу має бути тісно інтегрована з регістром ризиків ІБ , що дозволяє: зіставляти реальні інциденти з теоретичною моделлю ризиків; періодично оновлювати рівні P (ймовірність) та I (вплив); забезпечувати циклічність процесу управління ризиками (risk management loop).

Після запровадження комплексної системи моніторингу ДСБТ зможе: зменшити час виявлення та усунення інцидентів на 25-40%; забезпечити прозорість процесів інформаційної безпеки; своєчасно реагувати на критичні

інциденти; підвищити загальну стійкість цифрових сервісів та реєстрів; покращити відповідність вимогам КСЗІ та стандартам кіберзахисту; формувати лінійку доказів для внутрішнього та зовнішнього аудиту.

На рисунку подано типову архітектуру сучасної системи моніторингу безпеки, яка може бути адаптована для потреб ДСБТ.

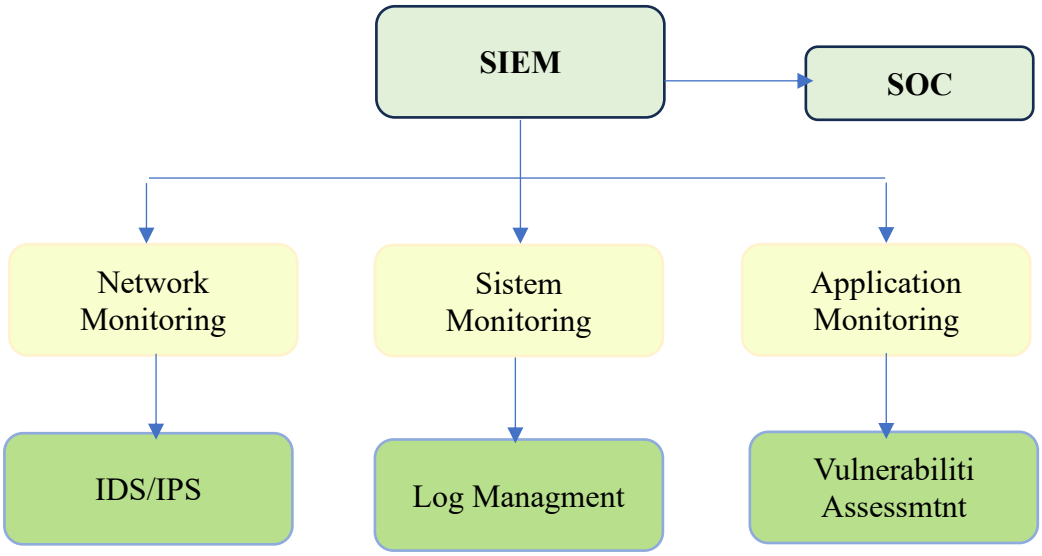

Рис. 3.3. Архітектура системи моніторингу та реагування на інциденти інформаційної безпеки

Представлена архітектура демонструє комплексний підхід до організації процесів моніторингу та реагування на інциденти. Її головним перевагою є централізоване об'єднання різнорідних джерел подій – серверів, мережевих пристроїв, застосунків, реєстрів та систем контролю – в єдину SIEM-платформу, що забезпечує глибоку кореляцію та аналітику загроз. Інтеграція з платформами реагування дозволяє не лише виявляти, а й оперативно локалізовувати інциденти. Використання SOC як фінального компонента гарантує цілодобовий моніторинг, аудит та аналіз безпекових подій, що суттєво підвищує зрілість системи кіберзахисту та знижує ризик критичних збоїв у роботі цифрових сервісів ДСБТ.

Функціональна модель SOC відображає системну організацію процесів зі збору, обробки, аналізу та реагування на події інформаційної безпеки в організації. Модель є багаторівневою та включає логічно пов'язані компоненти, які забезпечують неперервний моніторинг, раннє виявлення загроз, їх аналіз, а також координацію заходів протидії кіберінцидентам.

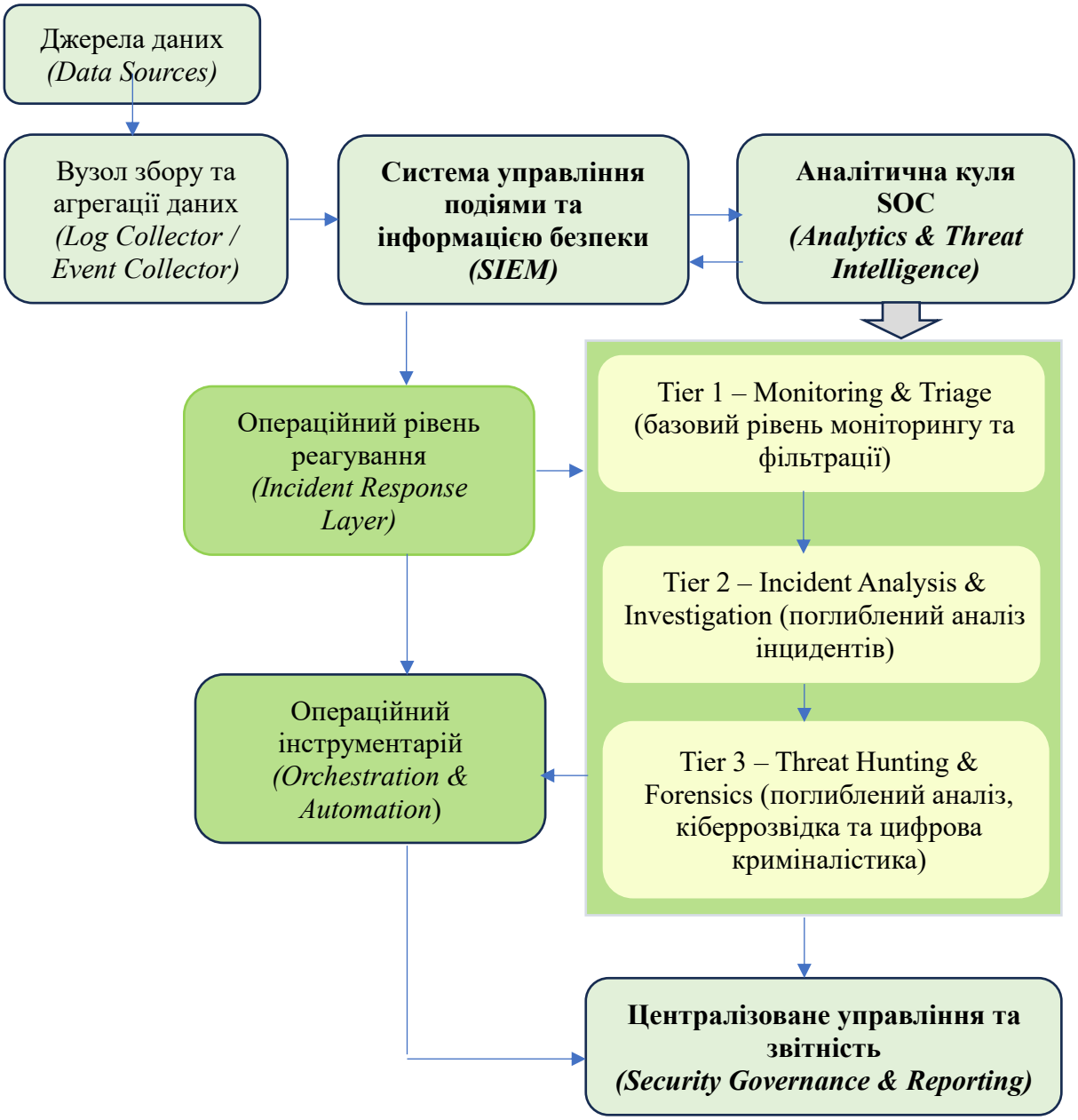

Рис. 3.4 Функціональна модель Центру оперативного реагування на інциденти безпеки (SOC)

Нижче наведено повне опис ключових функціональних елементів SOC.

1. Джерела даних (Data Sources). SOC отримує інформацію з великої кількості розподілених та гетерогенних джерел. Вони формують вхідний потік даних, який дає змогу відстежувати події в інформаційних системах у реальному часі. До таких джерел належить:

- Endpoint Devices – робочі станції, ноутбуки, мобільні пристрої, що генерують журнали подій, включаючи інформацію про доступи, задіяні процеси, зміни конфігурацій.

- Network Devices – маршрутизатори, комутатори, мережеві екрани, VPN-шлюзі, точки доступу Wi-Fi, що забезпечують дані про трафік, спроби проникнення, аномальні з'єднання.
- Cloud Services – хмарні платформи (SaaS, IaaS, PaaS), журнали аудиту, журнали активності користувачів.
- Applications – журнали роботи корпоративних застосунків, транзакційні логи, телеметрія модулів авторизації.
- Firewalls & IDS/IPS – інформація про блоковані спроби проникнення, виявлені експлойти, сканування портів.
- Security Tools – антивірусні системи, сканери уразливостей, системи аналізу поведінки користувачів (UEBA), які надають додаткову аналітику безпеки.

Джерела даних функціонують як сенсори безпеки, що забезпечують SOC актуальною інформацією для виявлення загроз.

2. Вузол збору та агрегації даних (Log Collector / Event Collector)

Цей компонент відповідає за приймання подій від усіх джерел, їх первичне опрацювання та трансформацію у стандартизований формат. Основні функції: нормалізація різнорідних форматів журналів; стиснення та оптимізація передачі даних; маршрутизація потоків у SIEM чи аналітичні модулі; фільтрація неважливих чи дубльованих подій. Цей рівень забезпечує масштабованість SOC та запобігає перевантаженню центральних аналітичних систем.

3. Система управління подіями та інформацією безпеки (SIEM). SIEM – ядро SOC, яке здійснює центральну кореляцію, аналіз та зберігання журналів подій.

Функції: автоматичне співставлення подій між різними джерелами; виявлення складних багатоступеневих атак (наприклад, lateral movement); застосування правил виявлення аномалій; створення сповіщень про підозрілі активності; формування історичних моделей загроз. SIEM дозволяє оперативно визначити інциденти, що потребують втручання аналітиків SOC.

4. Аналітична куля SOC (Analytics & Threat Intelligence). Цей рівень включає інструменти глибинного аналізу загроз. Складники:

- SOC Analysts – аналітики рівнів L1–L3, які досліджують події, класифікують інциденти, визначають рівень критичності та формують рекомендації.

- Threat Intelligence – використання даних про глобальні та локальні кіберзагрози: індикатори компрометації (IoC), тактики та методи атаки (MITRE ATT&CK), тренди кіберзлочинності.

- ML/AI models – автоматизовані алгоритми виявлення аномалій, поведінковий аналіз користувачів, прогнозування потенційних атак.

Tier 1 – Monitoring & Triage (базовий рівень моніторингу та фільтрації)

Аналітики першого рівня забезпечують первичну обробку подій безпеки, що включає перегляд і фільтрацію сповіщень SIEM, визначення їх пріоритетності, початкову кваліфікацію інцидентів та відбір випадків, які потребують поглибленого аналізу. У разі підтвердження ознак інциденту вони здійснюють ескалацію матеріалів на рівень Tier 2. Основна мета Tier 1 – відсіяти хибні спрацювання та визначити інциденти, які потребують розширеного розслідування.

Tier 2 – Incident Analysis & Investigation (поглиблений аналіз інцидентів) Аналітики другого рівня здійснюють поглиблене опрацювання інцидентів інформаційної безпеки, що охоплює детальний аналіз подій, вивчення логів, мережевого трафіку та поведінкових аномалій. Вони визначають масштаб, цілі та механізм кібератаки, ідентифікують ознаки компроментації (IoC) та тактики, техніки та процедури злодійника (TTP). На основі отриманих результатів фахівці оновлюють правила кореляції SIEM та конфігурації систем виявлення для мінімізації ризику повторних інцидентів. Діяльність цього рівня забезпечує комплексне розуміння характеру та джерела загрози.

Tier 3 – Threat Hunting & Forensics (поглиблений аналіз, кіберрозвідка та цифрова криміналістика). Аналітики третього рівня виконують найскладніші та найбільш ресурсоємні завдання у межах діяльності SOC. Їх робота включає проведення активних пошукових операцій з виявлення загроз (threat hunting), аналіз цільових та високотехнологічних кібератак типу APT, здійснення цифрової криміналістики та поглибленого аналізу шкідливого програмного

забезпечення. Крім того, фахівці цього рівня формують аналітичні звіти про загрози (threat intelligence) та розробляють нові механізми та правила детекції. У межах своєї компетенції вони також забезпечують удосконалення методології роботи SOC та систематичне розширення бази знань про загрози. Аналітичний рівень забезпечує можливість швидкого реагування та раннього виявлення складних загроз.

5. Операційний рівень реагування (Incident Response Layer)

Цей компонент охоплює процеси реагування на кіберінциденти та координацію дій щодо їх усунення. Функціональні завдання цього блоку включають класифікацію та пріоритезацію інцидентів, локалізацію порушень шляхом ізоляції уражених пристроїв або блокування облікових записів, усунення загроз та відновлення повноцінного функціонування інформаційних систем. Також передбачено взаємодію з відповідними органами державного рівня, зокрема CERT-UA та Держспецзв'язку, у разі виникнення інцидентів підвищеної критичності, а також обов'язкове документування всіх дій у системі управління інцидентами. Результатом функціонування цього компонента є забезпечення кіберстійкості організації.

6. Операційний інструментарій (Orchestration & Automation). Компоненти SOAR (Security Orchestration, Automation and Response) забезпечують автоматизоване реагування та підтримку процесів SOC. Основні можливості: автоматичне блокування IP-адрес, акаунтів або процесів; запуск сценаріїв реагування в разі повторюваних інцидентів; формування звітів та дашбордів; створення уніфікованих playbooks для різних типів атак. SOAR підвищує швидкість реагування та зменшує навантаження на аналітиків.

7. Централізоване управління та звітність (Security Governance & Reporting). Фінальний рівень моделі забезпечує управління всією системою, стратегічний контроль та вироблення політики інформаційної безпеки. Включає: KPI та KRI для оцінки ефективності SOC; стратегічне планування заходів кіберзахисту; формування регулярної звітності для керівництва; управління політиками доступу та нормативними вимогами; контроль

неперервності функціонування SOC**.** Цей рівень забезпечує інтеграцію SOC у загальну систему управління організацією.

Сукупність запропонованих рішень формує інтегровану модель кіберстійкості – від побудови єдиної системи управління ІБ до впровадження сучасних операційних практик та розвитку цифрової грамотності співробітників. Узагальнення результатів дає можливість оцінити очікуваний економічний, операційний та організаційний ефект.

Запропоновані у підрозділі 3.1 стратегічні та організаційні зміни спрямовані на формування цілісної моделі управління інформаційною безпекою ДСБТ. Основними елементами цієї моделі є: створення єдиної централізованої системи управління інформаційною безпекою (ISMS); уніфікація політик, регламентів і процедур у всіх структурних підрозділах; імплементація вимог міжнародних стандартів ISO/IEC 27001 та NIST; запровадження комплексної системи управління ризиками; а також формування централізованого реєстру інцидентів та вразливостей.

Хоча впровадження таких заходів не забезпечує негайного прямого фінансового результату, їх вплив проявляється у створенні передумов для суттєвого зниження неефективності внутрішніх процесів та ризиків інформаційної безпеки. Системність нових механізмів сприяє запобіганню повторюваним інцидентам, усуває дублювання функцій і зменшує кількість помилок, зумовлених відсутністю стандартизованих процедур.

Орієнтовні кількісні показники ефекту від реалізації стратегічних заходів включають:

зменшення адміністративних витрат на координацію та дублювання документації на 10-15%, що відповідає приблизно 70-110 тис. грн на рік;

зниження кількості інцидентів, спричинених нечіткістю або відсутністю процедур, на 5-8%, що становить додаткову економію на рівні ≈ 55-90 тис. грн щорічно;

підвищення ефективності реагування на інциденти завдяки унормованим процесам, що забезпечує скорочення часу аналізу на 20%.

Таким чином, стратегічні заходи створюють фундамент для розвитку зрілої системи інформаційної безпеки та формують мультиплікативний ефект, який підсилює результативність подальших технологічних і кадрових ініціатив.

Запропоновані у підрозділі 3.2 технологічні рішення спрямовані на зміцнення технічного контуру інформаційної безпеки ДСБТ. До ключових заходів цього напряму належать: впровадження центру моніторингу безпеки (SOC), використання системи централізованого кореляційного аналізу подій (SIEM), запровадження процедур управління вразливостями, розширення журналювання подій, застосування багатофакторної автентифікації (MFA), а також забезпечення безперервного моніторингу безпеки в режимі реального часу. Комплексна реалізація цих інструментів забезпечує суттєве підвищення здатності організації своєчасно виявляти та блокувати кібератаки, скорочувати час реагування на інциденти (MTTR), мінімізувати ймовірність компрометації IT-ресурсів і зменшувати витрати на відновлення після інцидентів середнього та високого рівня критичності. Таким чином, технологічні заходи створюють можливість переходу від реактивної до проактивної моделі кіберзахисту.

Економічний ефект від технологічних заходів

Технічні інциденти, пов’язані з порушеннями конфігурацій, експлуатацією вразливостей або спробами зовнішнього втручання, є значно дорожчими у ліквідації порівняно з інцидентами, спричиненими людським фактором. Середня вартість одного такого інциденту становить 3000-5000 грн, що охоплює витрати на відновлення систем, перевстановлення ПЗ, проведення аудитів, а також зниження продуктивності через вимушені простої.

Очікується, що впровадження SOC/SIEM дозволить зменшити кількість технічних інцидентів на 20-25% протягом першого року. За умови, що орієнтовна кількість таких інцидентів у ДСБТ становить близько 300 випадків на рік, економічний ефект можна визначити за формулою:

Економія = 300 × 25% × 4000 грн = 300 000 грн.

Таким чином, технологічні заходи забезпечують значний фінансовий ефект та формують стабільну основу для підвищення рівня кібервитривалості організації.

Стратегічні заходи (підрозділ 3.1) забезпечують оптимізацію управлінських процесів, уніфікацію документації та підвищення якості координації, що сприяє зменшенню адміністративних витрат і скороченню помилок, спричинених відсутністю стандартизованих процедур. Технологічні рішення (підрозділ 3.2) орієнтовані на підвищення здатності організації до проактивного виявлення інцидентів і мінімізації вартості їх ліквідації, що дає змогу зменшити частоту технічних інцидентів на 20-25%. Кадрові заходи (підрозділ 3.3), у свою чергу, забезпечують усунення найбільш поширених причин інцидентів – людських помилок – шляхом системного підвищення цифрової компетентності співробітників та формування ролевої моделі навчання.

Сумарна оцінка економічного ефекту, розрахована на підставі кількісних показників кожного напряму, наведена у таблиці 3.5.

Таблиця 3.5

Інтегральний економічний ефект від реалізації заходів

Напрям заходів	Орієнтовна економія / рік
Стратегічні та організаційні заходи (3.1)	120 000 – 200 000 грн
Технологічні заходи (3.2)	300 000 грн
Кадрові заходи та кібергігієна (3.3)	807 500 грн
Додатковий операційний ефект (зниження MTTR, оптимізація підтримки)	80 000 – 120 000 грн

Узагальнений розрахунок показує, що сумарний економічний ефект від упровадження запропонованих заходів становить:

Близько 1300000 – 1420000 грн на рік.

Це підтверджує, що комплексна трансформація системи інформаційної безпеки ДСБТ не лише підвищує рівень кіберстійкості, але й забезпечує відчутну економію ресурсів. Інтегральний ефект має мультиплікативний характер: стратегічні зміни підсилюють результативність технологічних заходів, а підвищення цифрової грамотності персоналу зменшує навантаження на технічні служби та знижує ймовірність повторних інцидентів. Таким чином, реалізація розробленої системи заходів є економічно обґрунтованою та сприяє сталому розвитку інфраструктури інформаційної безпеки ДСБТ.

Висновки до розділу 3:

Отже, підрозділ 3.1 визначив фундаментальні стратегічні напрями, які формують основу майбутньої системи інформаційної безпеки ДСБТ. Розроблення інтегрованої системи управління ІБ (ISMS), уніфікація регламентів, формування централізованого реєстру інцидентів, посилення ризик-менеджменту та впровадження міжнародних стандартів забезпечують перехід до цілісної керованої моделі. Стратегічні заходи створюють передумови для підвищення процесної зрілості, усувають фрагментованість підходів і забезпечують уніфіковану координацію між структурними підрозділами. Хоча їх вплив має переважно організаційний характер, результатом є скорочення адміністративних витрат, зменшення помилок та підвищення ефективності управлінських рішень у сфері ІБ.

Підрозділ 3.2 доводить, що модернізація технічної інфраструктури є ключовою умовою формування стійкої та керованої системи кіберзахисту. Впровадження SOC, SIEM, систем управління вразливостями, EDR/XDR, DLP, багатофакторної автентифікації та оновлених криптографічних стандартів забезпечує своєчасне виявлення, блокування та нейтралізацію загроз. Матриця пріоритетності дозволяє поетапно впроваджувати рішення, оптимізуючи ресурси та забезпечуючи поступовий перехід від базового рівня захисту до проактивної моделі. Удосконалення операційних процедур – журналювання, резервування, IRP/BCP, патч-менеджмент – підсилює ефективність технічних рішень, зменшує площину атаки та

Підрозділ 3.3 встановлює, що людський фактор є одним із головних чинників ризику для інформаційної безпеки ДСБТ. Запровадження системи регулярних тренінгів, ролевих програм, фішингових симуляцій, інформаційних кампаній, чеклістів та періодичного оцінювання знань забезпечує формування сталої культури кібергігієни. Комплексна система навчання охоплює всі категорії персоналу – від інспекторів до керівництва та забезпечує адаптивність до нових загроз. Вплив заходів проявляється у суттєвому зниженні частоти помилок користувачів, зменшенні рівня фішингових переходів і скороченні

кількості інцидентів, пов’язаних з необережними діями. У підсумку кадрові заходи становлять найбільший внесок у зниження ризикового навантаження.

Стратегічні заходи забезпечують економію на рівні 120- 200 тис. грн; технологічні рішення – близько 300 тис. грн за рахунок зменшення кількості технічних інцидентів; кадрові ініціативи – понад 807 тис. грн завдяки зниженню інцидентів людського фактору. Додатковий операційний ефект (зменшення MTTR, оптимізація реакції) формує ще 80-120 тис. грн економії. Сумарний інтегральний економічний ефект становить приблизно 1,3-1,42 млн грн на рік, що підтверджує раціональність інвестицій та синергійний характер запропонованих змін. Комплексний підхід дозволяє підсилити кожну групу заходів і створити стійку, масштабовану та економічно ефективну систему кіберзахисту.

Сформовано інтегровану модель удосконалення інформаційної безпеки ДСБТ, що поєднує стратегічну трансформацію, технічну модернізацію та підвищення компетентності персоналу. Системність підходу забезпечує не лише підвищення кіберстійкості та ефективності реагування, а й значну економію ресурсів та відповідність сучасним стандартам кіберзахисту. Реалізація запропонованих заходів створює передумови для переходу ДСБТ до рівня проактивного управління ІБ та формує основу для безпечної цифрової трансформації служби.

ВИСНОВКИ І ПРОПОЗИЦІЇ:

Магістерська робота присвячена комплексному дослідженню теоретичних, організаційних, правових, технічних та управлінських аспектів забезпечення інформаційної безпеки в системі публічного управління в умовах цифрової трансформації, а також формуванню та оцінюванню ефективності заходів щодо удосконалення механізмів ІБ на прикладі Державної служби України з безпеки на транспорті (ДСБТ). Проведене дослідження дає змогу сформулювати такі узагальнені висновки.

Доведено, що інформаційна безпека в системі публічного управління є багатовимірною категорією, яка охоплює правові, організаційні, технічні, кадрові та комунікаційні механізми, що забезпечують захист державних інформаційних ресурсів, стійкість інформаційно-комунікаційних систем та безперервність державних процесів. Установлено, що цифрова трансформація істотно змінює акценти в системі ІБ, переводячи її зі статусу допоміжного елементу у статус ключового чинника стійкості державного управління та національної безпеки. Посилення кіберзагроз, зростання ролі електронних реєстрів та інтегрованих інформаційних систем зумовлюють необхідність переходу до ризик-орієнтованої, адаптивної, багаторівневої моделі кіберзахисту.

Аналіз функціонування системи ІБ ДСБТ засвідчив, що в організації вже існує структурована основа для забезпечення ІБ – спеціалізовані підрозділи, внутрішні нормативні документи, канали взаємодії з національними центрами кіберзахисту, цифрові реєстри й сучасні інформаційні сервіси. Проте виявлені проблеми, такі як фрагментованість політик, різний рівень підготовки персоналу, недостатня інтегрованість систем та обмеженість ресурсів, стримують подальший розвиток та створюють додаткові ризики. Результати оцінювання стану ІБ показали, що технічні ризики (вразливості систем, атаки на мережеву інфраструктуру), організаційні (недостатня стандартизація процесів), кадрові та інтеграційні ризики є найбільш критичними.

Обґрунтовано необхідність модернізації системи інформаційної безпеки ДСБТ. Запропонований комплекс заходів охоплює стратегічний, організаційний,

технологічний та кадровий виміри: створення інтегрованої системи управління інформаційною безпекою (ISMS), удосконалення нормативного масиву, впровадження SOC/SIEM, розвиток криптографічного захисту, оптимізацію управління інцидентами, посилення навчання персоналу та формування культури кібергігієни. Особливу увагу приділено переходу до проактивного ризик-менеджменту та автоматизації процесів контролю.

Проведений економічний аналіз довів, що впровадження запропонованих заходів має чітко обґрунтований і значний інтегральний економічний ефект. Сумарна річна економія, сформована за рахунок зниження витрат на інциденти, оптимізації управлінських процесів, зменшення кількості помилок персоналу та підвищення ефективності реагування, становить близько 1,3-1,42 млн грн на рік. Доведено, що технологічні заходи (SOC/SIEM, моніторинг, MFA, управління вразливостями) є найбільш економічно результативними, але стратегічні та кадрові заходи формують мультиплікативний довгостроковий ефект, який підсилює загальну кіберстійкість установи.

Розроблена модель удосконалення механізмів забезпечення ІБ є комплексною, практично орієнтованою та придатною до впровадження у ДСБТ. Вона враховує сучасні стандарти та принципи кіберзахисту (ISO/IEC 27001, NIST CSF, GDPR), а також українські нормативні акти, що регулюють сферу інформаційної безпеки. Запропонована система дозволяє забезпечити керованість процесів ІБ, централізацію контролю, зниження ризиків людського фактору, підвищення прозорості, контрольованості та надійності функціонування інформаційних систем.

Отже, модернізація системи інформаційної безпеки ДСБТ є не лише актуальною, але й критично важливою передумовою забезпечення ефективного, безпечного та стійкого публічного управління в умовах цифрової трансформації та зростання кіберзагроз. Запропоновані заходи формують цілісну модель розвитку ІБ, яка поєднує стратегічні управлінські рішення, технологічні інновації та формування культури відповідальної поведінки персоналу, забезпечуючи підвищення рівня кіберстійкості та економічну доцільність їх впровадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. С. 141.

2. Про національну безпеку України: Закон України 21 червня 2018 року № 2469-VIII Відомості Верховної Ради (ВВР), 2018, № 31, ст.241 URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента від 28.12.2021 № 685/2021 URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

4. Засуха М. В. Сутність цифрової трансформації публічного управління // Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2024. №12. DOI: https://doi.org/10.54929/2786-5746-2024-12-02-04

5. Босак І. Інформаційна безпека України: загрози та методи протидії. Київський економічний науковий журнал. 2025. № 9. С. 33-38. DOI: https://doi.org/10.32782/2786-765X/2025-9-4.

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. С. 403.

7. Ангелін М. І. Формування механізмів інформаційного забезпечення публічного управління в Україні / М. І. Ангелін // Освітня аналітика України. 2025. № 2 (34). С. 81-90.

8. Квітка С., Новіченко Н., Гусаревич Н., Піскоха Н., Бардах О., Демошенко Г. Перспективні напрямки цифрової трансформації публічного управління // Аспекти публічного управління. № 8(4), 2020. С. 129-146. URL: https://aspects.org.ua/index.php/journal/article/view/807

9. Мінчеков А.Ю. Сутність поняття інформаційна безпека в сучасній науці публічного управління // Наукові перспективи. 2024. №4 (46). URL: http://perspectives.pp.ua/index.php/np/article/view/10972/11031.

10. Нагорняк М. М. Інформаційна безпека у системі публічного управління: виклики та перспективи / М. М. Нагорняк //Дніпровський науковий часопис публічного управління, психології, права. Випуск 1, 2024. С. 64-68
11. Лисенко С.О. Вдосконалення стратегічних принципів державного управління інформаційною безпекою у складі національної безпеки України // Актуальні проблеми у сфері публічного управління. Том 34 (73) № 1 2024. С. 311-316
12. Саричев Ю.О. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління. Вісник НАДУ при Президентові України (Серія «Державне управління»). 2017. № 3. С. 120-126.
13. Богом'я В. І., Черемісіна Л. О., Ярмолатій А. В., Галунько В.В. Ефективна організація системи стандартів та правових норм інформаційної безпеки: Водний транспорт: Збірник наукових праць. Випуск 1(42). 2025 https://vt.duit.in.ua/index.php/home/article/view/419/372
14. Галіпчак В. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. Науковий журнал «Політикус». 2023. № 5. С. 19-24.
15. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України: Указ Президента від 25.02.2017 № 47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text.
16. Бородін Є., Піскоха Н., Демошенко Г. Проблеми і переваги цифровізації місцевого самоврядування // Аспекти публічного управління. № 9(4), 2021. С. 95-103. URL: https://aspects.org.ua/index.php/journal/article/view/892
17. Горбата Л. Проблемні аспекти забезпечення інформаційної відкритості в умовах цифрової трансформації публічного управління. Публічне управління та місцеве самоврядування, Вип. 3, 2024, DOI: https://doi.org/10.32782/2414-4436/2024-3-1
18. Лопушинський І. П. «Цифровізація» як основа державного управління на шляху трансформації та реформування українського суспільства // Теорія та практика державного управління і місцевого самоврядування. 2018. № 2. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2018_2_20.

19. Макарова І. О. Цифровізація публічного управління на регіональному та міському рівнях / І. О. Макарова, Ю. Б. Пігарєв, Л. С. Сметаніна // Актуальні проблеми державного управління : зб. наук. пр. ОРІДУ. 2021. №. 2(83). С. 86 - 91.

20. Савченко О.С. Систематизація наукових підходів до поняття «цифровізація у публічному управлінні» Держава та регіони. Серія: Публічне управління і адміністрування, 2022 р., № 2 (76). С. 72-76 DOI https://doi.org/10.32840/1813-3401.2022.2.12

21. Босак І. Інформаційна безпека України: загрози та методи протидії. Київський економічний науковий журнал. 2025. № 9. С. 33-38. DOI: https://doi.org/10.32782/2786-765X/2025-9-4.

22. Горулько В.В. Основні напрями удосконалення законодавства України з інформаційної безпеки в умовах війни // Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Випуск 88: частина 2. С. 364-368.

23. Малий І. Й., Цедік М. Г. Інституційний вимір цифровізації державного управління в Україні // Державне управління: удосконалення та розвиток. 2022. № 2. DOI: https://doi.org/10.32702/2307-2156-2022.2.3.

24. Кобець Т. Аналіз загроз когнітивній безпеці українського суспільства: класифікаційні підстави. 2024. С. 67-72. URL: https://journals.pnu.if.ua/index.php/politology/article/view/182/178.

25. Рейндам Р. К. Інформаційна безпека в системі публічного управління: проблеми та вирішення / Р. К. Рейндам ; наук. керівник Д. А. Терещенко // Молодіжний соціологічний форум НТУ «ХПІ»: матеріали міжнар. наук.-практ. конф. студентів і аспірантів, присвяченої 140-річчю Національного технічного університету «Харківський політехнічний інститут», 16 травня 2025 р., м. Харків, Україна / редкол.: Мороз В. М., Круглов В. В., Бірюкова М. В. [та ін.]; Нац. техн. ун-т «Харків. політехн. ін-т» [та ін.]. Харків: НТУ «ХПІ», 2025. С. 136-140. URI https://repository.kpi.kharkov.ua/handle/KhPI-Press/90980

26. Сердюк І.А. Підходи публічного управління до інформаційної безпеки особистості. Публічне урядування. 2022. № 3 (31). С. 53-59. DOI: https://doi.org/10.32689/2617-2224-2022-3(31)-7

27. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право». 2020. Випуск 29. С. 281-288. DOI: https://doi.org/10.26565/2075-1834-2020-29-38

28. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління / Я. І. Чмир // Аспекти публічного управління. - 2018. Т. 6, № 9. С. 16-22. URL: http://nbuv.gov.ua/UJRN/aplup_2018_6_9_4

29. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT) URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795

30. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon. rada.gov.ua/laws/show/2163-19.

31. Запорожець С. Інформаційна безпека України в умовах гібридної війни. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2019. № 17. С. 52-63. URL: https://doi.org/10.46972/2076-1546.2019.17.05.

32. Захаренко, К. Розвиток системи інформаційної безпеки: досвід зарубіжних країн [Текст] / К. Захаренко // Вища освіта України. 2018. № 3. С. 71-77.

33. Золотар О.О. Особливості інформаційної безпеки людини в умовах гібридної війни // Інститут інформації, безпеки і права НАПрН України, 2021. С. 25-30.

34. Пригожин А. О. Проблеми доступу до публічної інформації та інформаційна безпека в публічному управлінні // Наукові інновації та передові технології. 2025. № 2(42). DOI: 10.52058/2786-5274-2025-2(42).

35. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. № 48. С. 650.

36. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» Указ Президента України 6 серпня 2021 року № 447/2021 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
37. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони»: Указ Президента України 18 червня 2021 року № 260/2021 URL: https://zakon.rada.gov.ua/laws/show/260/2021#Text
38. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках: Розпорядження Кабінету Міністрів України від 31 грудня 2024 р. № 1351-р URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text
39. Al-Ansi A. M., Al Ansi A. M., Garad A., Jaboob M., Al-Ansi A. Elevating e-government: Unleashing the power of AI and IoT for enhanced public services // Heliyon. 2024. Vol. 10, No. 23. P. e40591. DOI: 10.1016/j.heliyon.2024.e40591.
40. Arifkhodzhaieva T. Digitalisation and counteraction to information threats in the state security management system // Visegrad Journal on Human Rights. 2024. No. 5. P. 6-12. DOI: 10.61345/1339-7915.2024.5.1.
41. de Araujo M. S., Souza Machado B. A., Passos F. U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance // Applied Sciences. 2024. Vol. 14, No. 5. P. 2116. DOI: 10.3390/app14052116.
42. Lizut R. Security challenges of IoT integration in national and state critical infrastructures // Politics & Security. 2025. Vol. 13, No. 3. P. 82–94. DOI: 10.54658/ps.28153324.2025.13.3.pp.82-94.
43. Mushtaq, S., & Shah, M. (2024). Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. Information, 2024. 15(10), 619. https://doi.org/10.3390/info15100619

44. Sun Y., Zhang Y.-F., Wang Y., Zhang S. Cooperative governance mechanisms for personal information security: an evolutionary game approach // Kybernetes. 2023. Ahead-of-print. DOI: 10.1108/K-04-2023-0717.
45. https://dsbt.gov.ua/pro-sluzhbu/struktura - офіційний сайт Державної служби з безпеки на транспорті/ Структура

ДОДАТКИ