МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ
ФАКУЛЬТЕТ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ
КАФЕДРА ДЕРЖАВНОЇ БЕЗПЕКИ

«МАГІСТЕРСЬКА РОБОТА ЗА ФАХОМ»

Роль інформаційної безпеки у державному секторі

здобувача вищої освіти
другого (магістерського) рівня вищої
освіти освітньо-професійної програми
251 «Державна безпека»
Герасименка Ігоря Олександровича
Науковий керівник:
Мальцев Віталій Вікторович,
кандидат юридичних наук,
старший дослідник,
професор кафедри соціально-гуманітарних
дисциплін факультету забезпечення
державної безпеки Київського інституту
Національної гвардії України

Магістерська робота захищена
з оцінкою_____
«___»_____ 2026 р.

Київ – 2026

АНОТАЦІЯ

Герасименко Ігор Олександрович «Роль інформаційної безпеки у державному секторі» – Рукопис.

Магістерська робота присвячена дослідженню проблем забезпечення інформаційної безпеки в державному секторі України в умовах цифровізації, зростання кіберзагроз та гібридних інформаційних впливів. У роботі обґрунтовано актуальність інформаційної безпеки як ключової складової національної безпеки та необхідної умови ефективного функціонування органів державної влади.

Метою дослідження є комплексний аналіз сучасного стану інформаційної безпеки в державному секторі України та розробка практично орієнтованих напрямів її вдосконалення. Об’єктом дослідження є інформаційна безпека як елемент системи державного управління та національної безпеки. Предметом дослідження виступає система забезпечення інформаційної безпеки в державному секторі України, зокрема її правові, організаційні, технологічні та управлінські аспекти.

У процесі дослідження застосовано методи логічного й системного аналізу, порівняльно-правовий та нормативно-правовий аналіз, статистичні методи, кейс-метод аналізу кіберінцидентів, а також елементи моделювання сценаріїв розвитку інформаційних загроз. Це дало змогу комплексно оцінити ефективність чинної системи забезпечення інформаційної безпеки.

У роботі проаналізовано нормативно-правову базу України у сфері інформаційної та кібербезпеки, визначено основні загрози інформаційній безпеці державного сектору, зокрема кібератаки на інформаційні ресурси, витоки персональних і службових даних, вплив людського фактору та інформаційно-психологічні операції. Виявлено ключові проблеми функціонування системи інформаційної безпеки, серед яких фрагментарність законодавства, недостатня координація між державними органами, обмеженість ресурсів і кадровий дефіцит.

Наукова новизна отриманих результатів полягає в комплексному підході до оцінки інформаційної безпеки державного сектору з урахуванням сучасних кіберзагроз та гібридних впливів, а також у формуванні системи практичних рекомендацій щодо вдосконалення правового, організаційного та технологічного забезпечення інформаційної безпеки.

Практичне значення результатів дослідження полягає в можливості використання запропонованих рекомендацій у діяльності органів державної влади під час розроблення та реалізації стратегій і програм у сфері інформаційної та кібербезпеки.

Ключові слова:

інформаційна безпека, державний сектор, кібербезпека, державне управління, національна безпека, інформаційні загрози, захист інформації.

ABSTRACT

The master's thesis is devoted to the study of issues related to ensuring information security in the public sector of Ukraine under conditions of digitalization, the growing number of cyber threats, and hybrid information influences. The relevance of the research is substantiated by the role of information security as a key component of national security and a necessary condition for the effective functioning of public authorities.

The purpose of the study is to conduct a comprehensive analysis of the current state of information security in the public sector of Ukraine and to develop practically oriented directions for its improvement. The object of the research is information security as an element of the public administration system and national security. The subject of the research is the system of information security provision in the public sector of Ukraine, including its legal, organizational, technological, and managerial aspects.

The research methodology includes methods of logical and systemic analysis, comparative legal and regulatory analysis, statistical methods, a case-study approach to the analysis of cyber incidents, as well as elements of scenario modeling of information threats. This methodological framework made it possible to comprehensively assess the effectiveness of the existing information security system.

The thesis analyzes the legal and regulatory framework of Ukraine in the field of information and cybersecurity and identifies the main threats to information security in the public sector, including cyberattacks on information resources, leakage of personal and official data, the impact of the human factor, and information and psychological operations. Key problems in the functioning of the information security system are identified, such as the fragmentation of legislation, insufficient coordination among public authorities, limited financial and human resources, and a shortage of qualified cybersecurity personnel.

The scientific novelty of the research lies in a comprehensive approach to assessing information security in the public sector, taking into account modern cyber threats and hybrid influences, as well as in the development of a system of practical recommendations aimed at improving the legal, organizational, and technological support of information security.

The practical significance of the research results consists in the possibility of using the proposed recommendations in the activities of public authorities when developing and implementing strategies and programs in the field of information and cybersecurity.

Keywords:

information security, public sector, cybersecurity, public administration, national security, information threats, information protection.

ЗМІСТ

ВСТУП

У сучасному світі інформація стала одним із найважливіших ресурсів, який визначає рівень розвитку суспільства та держави. Процеси глобалізації, цифровізації та активного впровадження інформаційно-комунікаційних технологій суттєво трансформували всі сфери суспільного життя, включно з державним управлінням. Державний сектор, будучи ключовим інститутом управління суспільними процесами, дедалі більше залежить від надійного функціонування інформаційних систем, які забезпечують взаємодію органів влади, зберігання та обробку даних, а також доступ громадян до адміністративних послуг. Саме тому питання забезпечення інформаційної безпеки стає не лише технічним завданням, але й складовою національної безпеки.

Інформаційна безпека у державному секторі охоплює комплекс організаційних, правових та технічних заходів, спрямованих на захист інформаційних ресурсів від несанкціонованого доступу, спотворення, втрати чи знищення. Водночас слід відзначити, що в умовах гібридних загроз, кібератак на критичну інфраструктуру та активізації інформаційних воєн, забезпечення ефективного функціонування систем інформаційної безпеки в державних установах набуває стратегічного значення. Ця проблематика має не лише науковий, але й практичний вимір, адже від надійності захисту інформації залежить стабільність державного управління, довіра громадян до інститутів влади та конкурентоспроможність країни на міжнародній арені.

Актуальність теми дослідження зумовлена тим, що сучасні державні органи функціонують в умовах зростання кількості та складності кіберзагроз. Україна, зокрема, постійно стикається з кібератаками на державні інформаційні ресурси, системи управління інфраструктурою та бази персональних даних громадян. Прикладом є масштабні кібератаки на енергетичні компанії, державні

реєстри, сайти органів влади, які продемонстрували високий рівень вразливості національної інформаційної інфраструктури. Це свідчить про необхідність розробки ефективної системи захисту інформації, удосконалення законодавчої бази, формування стратегії кіберзахисту та посилення міжнародного співробітництва у цій сфері. Крім того, актуальність обраної теми підсилюється сучасними тенденціями цифровізації державних послуг («держава у смартфоні»), що вимагає від державного сектору особливої уваги до питань захисту інформації.

Мета дослідження полягає у комплексному аналізі ролі інформаційної безпеки в державному секторі, виявленні основних проблем і загроз, які перешкоджають ефективному функціонуванню системи захисту інформації, а також у розробці практичних рекомендацій щодо підвищення рівня інформаційної безпеки в органах державної влади України.

Для досягнення поставленої мети в роботі передбачено виконання таких **завдань**:

— розкрити сутність поняття «інформаційна безпека» та її значення у державному секторі;
— здійснити критичний аналіз наукових підходів до проблеми інформаційної безпеки;
— дослідити нормативно-правову базу України у сфері інформаційної безпеки та визначити її відповідність міжнародним стандартам;
— проаналізувати сучасні загрози й виклики, що постають перед державним сектором у сфері інформаційної безпеки;
— оцінити стан і практику забезпечення інформаційної безпеки в діяльності органів влади України;
— виявити недоліки у функціонуванні існуючої системи захисту;
— запропонувати напрями вдосконалення законодавчої, організаційної та технічної складових інформаційної безпеки.

Об’єкт дослідження: інформаційна безпека як складова державного управління та національної безпеки.

Предмет дослідження: система забезпечення інформаційної безпеки у державному секторі України, зокрема її правові, організаційні, технологічні та практичні аспекти.

У процесі дослідження застосовуються **різноманітні методи** наукового аналізу. Використано методи логічного та системного аналізу для розкриття сутності інформаційної безпеки; метод порівняльного аналізу для зіставлення української практики із міжнародним досвідом; нормативно-правовий аналіз для вивчення законодавчих актів; статистичний метод для оцінки масштабів загроз та ефективності застосованих заходів; кейс-метод для дослідження конкретних прикладів кіберінцидентів у державному секторі. Крім того, у роботі застосовуються методи моделювання для прогнозування можливих сценаріїв розвитку ситуації у сфері інформаційної безпеки.

Наукова новизна роботи полягає у поглибленому теоретичному осмисленні ролі інформаційної безпеки в державному секторі в умовах цифрової трансформації суспільства та в розробці практичних рекомендацій щодо вдосконалення існуючої системи її забезпечення в Україні. В роботі сформульовано авторське бачення шляхів гармонізації національного законодавства з міжнародними нормами, а також визначено інноваційні підходи до організації захисту державних інформаційних ресурсів.

Практичне значення отриманих результатів полягає у можливості їх використання органами державної влади при формуванні та реалізації політики інформаційної безпеки, у підвищенні ефективності роботи державних інформаційних систем, а також у підготовці та навчанні державних службовців у сфері інформаційної безпеки. Запропоновані рекомендації можуть стати основою для вдосконалення державних програм кіберзахисту та розробки нових стратегій, спрямованих на забезпечення стабільності та безпеки функціонування державного сектору в інформаційному суспільстві.

Структура роботи: робота складається зі вступу, чотирьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи – … сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДЕРЖАВНОМУ СЕКТОРІ

1.1. Поняття, сутність та основні принципи інформаційної безпеки

Поняття інформаційної безпеки сформувалося як результат розвитку інформаційного суспільства та зростання значення інформаційних ресурсів для функціонування держави, економіки та соціальних інститутів. В умовах глобальної цифровізації інформація перестала бути лише допоміжним елементом управлінської чи виробничої діяльності, а перетворилася на стратегічний ресурс, який забезпечує розвиток суспільства, стабільність державних механізмів і конкурентоспроможність країни у світовій спільноті. Саме тому категорія «інформаційна безпека» набула багатогранного змісту й стала предметом дослідження в правовій, політичній, технічній та управлінській науках.

У науковій літературі існує значна кількість визначень інформаційної безпеки, що відображають різні підходи до розуміння її сутності. У найбільш загальному вигляді інформаційну безпеку можна трактувати як стан захищеності інформації, інформаційних процесів і систем від загроз, що можуть призвести до порушення конфіденційності, цілісності чи доступності даних. Це означає, що інформаційна безпека полягає не лише в технічному захисті інформаційних систем від несанкціонованого доступу, а й у забезпеченні комплексного захисту всіх інформаційних ресурсів держави та суспільства.

Міжнародна організація зі стандартизації (ISO), зокрема в стандарті ISO/IEC 27001, визначає інформаційну безпеку як забезпечення збереження трьох ключових властивостей інформації: конфіденційності, що означає доступність інформації лише для уповноважених осіб; цілісності, яка передбачає

захист від несанкціонованих змін або спотворення; та доступності, тобто можливості використання інформації уповноваженими користувачами в необхідний час. Це визначення отримало широке визнання, оскільки відображає практичний підхід до управління інформаційною безпекою та створює основу для розробки універсальних стандартів у цій сфері.

Вітчизняні науковці, також, пропонують різні підходи до трактування поняття інформаційної безпеки. Частина з них акцентує увагу на державному вимірі цього феномену, розглядаючи інформаційну безпеку як здатність держави забезпечити захист інформаційних ресурсів, інфраструктури та інформаційних прав громадян від загроз як внутрішнього, так і зовнішнього походження. Інші дослідники підкреслюють соціальний аспект, відзначаючи, що інформаційна безпека включає також захист суспільства від інформаційної агресії, маніпуляцій та деструктивного інформаційного впливу, який може негативно позначатися на громадській думці, політичній стабільності чи національній ідентичності.

В контексті державного сектору інформаційна безпека розглядається як невід'ємний елемент системи національної безпеки, який забезпечує стабільність функціонування органів державної влади, збереження державних інформаційних ресурсів та захист стратегічно важливих даних від кіберзагроз. В цьому випадку вона включає не лише технічні та організаційні заходи захисту, але й правове регулювання, міжнародну співпрацю, кадрове забезпечення та формування культури безпечного використання інформаційних технологій серед державних службовців.

Розкриття сутності та концепцій інформаційної безпеки дає підстави стверджувати, що її ефективність залежить не лише від наявності законодавчих механізмів чи технічних рішень, а й від правильно вибудованої системи базових орієнтирів, які визначають логіку, послідовність і цілісність усіх заходів у цій сфері. Такими орієнтирами виступають принципи забезпечення інформаційної безпеки. Вони формують основу для розробки національних стратегій, створення нормативно-правових актів, вибору організаційних моделей управління інформаційними ресурсами та впровадження технологічних інструментів

захисту. Іншими словами, принципи інформаційної безпеки є своєрідними правилами, дотримання яких дозволяє державі, суспільству й окремим інституціям протидіяти загрозам і водночас створювати стабільне та безпечне інформаційне середовище.

Провідним серед цих принципів є принцип комплексності, який полягає у необхідності застосування взаємопов'язаних і взаємодоповнюючих заходів різного характеру — правових, організаційних, технічних, кадрових та освітніх. Жоден із цих напрямів не може гарантувати достатній рівень безпеки сам по собі, адже інформаційні загрози є багатогранними і динамічними. Тільки цілісна система, що поєднує різні підходи, здатна забезпечити належний рівень захищеності державних інформаційних ресурсів.

Не менш важливим є принцип безперервності, який відображає динамічну природу інформаційних загроз. Загрози змінюються, видозмінюються та вдосконалюються одночасно з розвитком технологій, тому забезпечення безпеки не може бути одноразовим актом. Це постійний процес моніторингу, виявлення нових ризиків, аналізу їх потенційного впливу та адаптації існуючих заходів захисту. Державний сектор у цьому контексті повинен мати механізми гнучкого реагування на інциденти та систему стратегічного прогнозування.

Особливу увагу слід приділити принципу законності. У сфері інформаційної безпеки він означає, що будь-які заходи із захисту інформації мають здійснюватися на основі чітко визначених законодавчих норм і не порушувати конституційних прав громадян. Цей принцип забезпечує баланс між захистом державних інтересів та збереженням демократичних цінностей, зокрема права на доступ до інформації, свободи слова й захисту персональних даних.

Принцип відповідальності визначає, що кожен учасник інформаційних відносин — від державних органів до окремих посадових осіб — має чітко усвідомлювати власні обов'язки у сфері захисту інформації. Він передбачає встановлення персональної відповідальності за порушення вимог інформаційної

безпеки, що стимулює дисципліну та сприяє зниженню ризику людського фактору, який часто є причиною вразливостей у системах.

Важливим орієнтиром виступає і принцип пропорційності, який полягає в оптимальному співвідношенні між витратами на захист і потенційними наслідками реалізації загроз. У державному секторі, де обмеженість ресурсів є особливо відчутною, цей принцип дозволяє визначати пріоритети, концентруючи зусилля на найбільш критичних об'єктах та інформаційних ресурсах.

Ключовим є й принцип міжнародної співпраці. Інформаційні загрози мають глобальний характер і часто виходять за межі окремих країн. Тому держави, зокрема й Україна, повинні координувати свої дії, обмінюватися досвідом, інформацією про кіберінциденти та спільно розробляти механізми протидії новим викликам. Реалізація цього принципу дозволяє інтегрувати національну систему інформаційної безпеки у ширший міжнародний контекст і використовувати кращі практики світового рівня.

Але, розуміння цих принципів набуває особливої ваги лише тоді, коли вони розглядаються у зв'язку з практикою державного управління. Саме в цій площині інформаційна безпека виявляє своє ключове значення, адже від її стану залежить не лише ефективність функціонування окремих інституцій, але й стабільність усього державного механізму, а отже — безпека та розвиток суспільства загалом.

Державне управління у XXI столітті ґрунтується на активному використанні інформаційно-комунікаційних технологій. Електронні реєстри, цифрові сервіси, автоматизовані системи управління процесами, бази даних персональної та службової інформації стали невід'ємною складовою діяльності органів влади. У такій ситуації будь-яке порушення цілісності, доступності чи конфіденційності інформації прямо впливає на здатність державних органів виконувати свої функції. Для прикладу, збої в роботі електронних систем податкової служби чи реєстраційних баз не лише створюють незручності для громадян і бізнесу, а й можуть завдати відчутних економічних збитків, знизити рівень довіри до держави та спричинити політичні наслідки.

Інформаційна безпека є також визначальним чинником у забезпеченні національної безпеки. Органи державної влади акумулюють у своїх системах величезні обсяги даних, у тому числі ті, що стосуються обороноздатності, економічної стратегії, дипломатичних відносин чи персональних даних громадян. Несанкціонований доступ до таких відомостей може поставити під загрозу життєво важливі інтереси держави, порушити баланс сил у міжнародних відносинах і навіть стати передумовою кризових ситуацій. Саме тому питання інформаційної безпеки у сфері державного управління розглядаються як складова частина стратегії національної безпеки та оборони.

Важливим аспектом є й те, що інформаційна безпека прямо впливає на якість прийняття управлінських рішень. Державні органи базують свою діяльність на аналітиці, яка формується з використанням інформаційних систем і баз даних. Якщо ці дані будуть спотворені або знищені, управлінські рішення можуть виявитися неефективними або навіть деструктивними. В умовах сучасних інформаційних воєн особливої актуальності набуває питання протидії маніпуляціям, дезінформації та кібератакам, які здатні впливати на стратегічні рішення державного рівня.

Не менш суттєве значення інформаційної безпеки полягає у формуванні довіри громадян до державних інституцій. Сучасна держава активно розвиває електронне урядування, надає послуги онлайн, переводить значну частину документообігу в цифрову форму. Якщо громадяни не будуть впевнені у захищеності своїх персональних даних, вони сприйматимуть державні цифрові сервіси як потенційно небезпечні. Це призведе до зниження їх популярності, гальмування цифровізації та збереження корупційних ризиків у традиційних паперових процедурах. Тому інформаційна безпека виступає умовою ефективного впровадження концепції «держава у смартфоні» та розвитку електронної демократії.

Окрім того, слід зазначити, що інформаційна безпека у сфері державного управління виконує ще й функцію кадрового та інституційного розвитку. Вона стимулює державні органи до формування нових структур, створення

спеціалізованих підрозділів із кіберзахисту, підготовки та перепідготовки державних службовців. Тому, розвиток системи інформаційної безпеки сприяє підвищенню професійного рівня управлінських кадрів, впровадженню сучасних стандартів управління та формуванню нової управлінської культури, орієнтованої на безпеку й стабільність.

Узагальнюючи, можна стверджувати, що значення інформаційної безпеки для державного управління є комплексним і багаторівневим. Вона забезпечує стійкість функціонування державних інституцій, захищає стратегічні інтереси країни, підвищує якість управлінських рішень, формує довіру громадян до державних сервісів і стимулює розвиток інституційної спроможності держави. Саме тому питання інформаційної безпеки повинні розглядатися не як технічне завдання, а як стратегічний пріоритет державної політики, від якого залежить ефективність та стабільність усього механізму державного управління.

1.2. Нормативно-правове забезпечення інформаційної безпеки в державному секторі

Розуміння ролі інформаційної безпеки у державному секторі неможливе без аналізу нормативно-правового підгрунтя, яке визначає правила функціонування систем захисту інформації та окреслює вимоги до органів влади, відповідальних за їхню реалізацію. Правове регулювання у цій сфері має багаторівневу структуру: воно охоплює як міжнародні стандарти й угоди, що задають універсальні підходи до організації інформаційної безпеки, так і національне законодавство, яке враховує особливості внутрішньої політичної, економічної та безпекової ситуації в країні.

У міжнародній практиці ключову роль відіграють стандарти, розроблені Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Найбільш відомим серед них є стандарт ISO/IEC 27001, що визначає вимоги до системи управління інформаційною безпекою (Information Security Management System — ISMS). Він встановлює

рамки для створення, впровадження, моніторингу та постійного вдосконалення процесів забезпечення захищеності інформаційних ресурсів. Особливе значення має те, що ISO/IEC 27001 орієнтує організації на управління ризиками, пов'язаними з інформаційними загрозами, що дозволяє будувати гнучкі й адаптивні системи захисту.

Додатково у міжнародному контексті важливими є стандарти ISO/IEC 27002, які пропонують практичні рекомендації з реалізації заходів безпеки, та ISO/IEC 27005, що регламентує управління ризиками інформаційної безпеки. Ці документи формують своєрідну методологічну базу, на яку орієнтуються держави при створенні власних національних систем кіберзахисту. Водночас варто згадати і стандарти Європейського Союзу, зокрема Директиву NIS (Network and Information Systems Directive), яка встановлює мінімальні вимоги до захисту критичних інформаційних систем і накладає обов'язки на держави-члени щодо створення органів кібербезпеки, механізмів обміну інформацією та реагування на інциденти.

Окрім стандартів, міжнародні організації формують політичні та правові рамки забезпечення інформаційної безпеки. Наприклад, НАТО активно розвиває концепцію кібероборони, розглядаючи кіберпростір як окремий домен ведення воєнних дій поряд із сушею, морем, повітрям і космосом. Для України це особливо важливо, оскільки співпраця з Альянсом відкриває доступ до передових методик і практик кіберзахисту. Подібну роль відіграє й діяльність Організації Об'єднаних Націй, яка у своїх резолюціях визначає принципи відповідальної поведінки держав у кіберпросторі.

Національне законодавство України у сфері інформаційної безпеки сформоване на основі міжнародних підходів, але водночас воно враховує особливості внутрішнього розвитку та специфіку загроз, з якими стикається країна. Конституція України закріплює право громадян на захист персональних даних та на доступ до інформації, що створює правову основу для подальшого розвитку галузевого законодавства. Базовим документом у цій сфері є Закон України «Про національну безпеку України», де інформаційна безпека

визначається як один із ключових елементів національної безпеки, а держава зобов’язується створювати умови для її забезпечення.

Важливе значення має також Закон України «Про інформацію», який встановлює загальні принципи інформаційних відносин, визначає права й обов’язки учасників, регламентує питання доступу до інформації та її захисту. Окремим напрямом правового регулювання є захист персональних даних, закріплений у Законі України «Про захист персональних даних». Він визначає механізми обробки, зберігання та використання даних громадян, орієнтуючись на стандарти Європейського Союзу, зокрема Загальний регламент захисту даних (GDPR).

Ключовим спеціалізованим документом у сфері кіберзахисту є Закон України «Про основні засади забезпечення кібербезпеки України». В ньому закріплено поняття кібербезпеки, визначено коло суб’єктів, відповідальних за її забезпечення, та окреслено систему координації діяльності у сфері захисту критичної інформаційної інфраструктури. Цей закон створює інституційне підгрунтя для функціонування таких структур, як Державна служба спеціального зв’язку та захисту інформації України, Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони, а також визначає роль Служби безпеки України та інших силових відомств у протидії кіберзагрозам.

Крім зазначених законів, існує низка підзаконних нормативно-правових актів, постанов уряду та відомчих інструкцій, які деталізують порядок застосування технічних і організаційних заходів. Наприклад, Державні стандарти України (ДСТУ), що гармонізовані з міжнародними, регулюють питання криптографічного захисту, управління ризиками та впровадження систем управління інформаційною безпекою.

Правове забезпечення інформаційної безпеки в Україні має багаторівневу структуру. На конституційному рівні закріплено основоположні принципи, які визначають інформаційні права громадян. Конституція гарантує право на свободу слова, право на інформацію та право на захист персональних даних. Ці положення створюють фундамент, на якому будується вся система

нормативного регулювання. Однак саме баланс між правами людини й обов’язком держави забезпечити інформаційну безпеку часто стає предметом дискусій, адже надмірна централізація функцій захисту може призвести до обмеження демократичних свобод.

На рівні спеціального законодавства ключову роль відіграють закони, які визначають правові основи функціонування інформаційних відносин. Закон України «Про інформацію» встановлює правові засади доступу до інформації, її використання та захисту. Він визначає категорії інформації з обмеженим доступом, серед яких державна таємниця, службова та комерційна інформація. Водночас практика його застосування свідчить, що інколи ці обмеження можуть використовуватися для приховування суспільно важливих відомостей, що породжує конфлікти між принципом відкритості й вимогами безпеки.

Закон України «Про захист персональних даних» є ще одним важливим елементом правового поля. Його положення спрямовані на забезпечення дотримання прав громадян під час обробки їхніх даних у державних і приватних структурах. Хоча він орієнтований на європейські стандарти, зокрема на Загальний регламент захисту даних (GDPR), у практиці його реалізації залишаються значні прогалини. Часто відсутні дієві механізми контролю за обробкою даних, а санкції за порушення залишаються недостатньо суворими, щоб забезпечити ефективне дотримання норм.

Надзвичайно важливим для аналізу є Закон України «Про основні засади забезпечення кібербезпеки України». Він закріплює визначення кібербезпеки та кіберзахисту, визначає суб’єктів, відповідальних за їх забезпечення, та створює основу для формування національної системи кіберзахисту. Однак реальна ефективність цього закону залежить від практичного наповнення його положень. На сьогодні координація між різними державними органами залишається недостатньо відпрацьованою, а розподіл повноважень часто призводить до дублювання функцій або, навпаки, до утворення «прогалин» у сфері відповідальності.

Правові аспекти інформаційної безпеки проявляються й у сфері захисту державної таємниці. Закон України «Про державну таємницю» регламентує порядок віднесення інформації до категорії секретної, визначає процедури її зберігання та використання. Водночас у сучасних умовах гібридної війни й масових кібератак класичні підходи до секретності потребують перегляду. Інформація, яка формально не належить до державної таємниці, але стосується функціонування критичної інфраструктури, може становити значний інтерес для зловмисників.

Варто підкреслити, що важливим аспектом правового регулювання є не лише наявність законодавчих актів, а й їхня відповідність міжнародним зобов'язанням України. Як країна, що прагне інтеграції до Європейського Союзу, Україна повинна гармонізувати своє законодавство зі стандартами ЄС. Це стосується не тільки захисту персональних даних, а й питань кібербезпеки, захисту критичної інформаційної інфраструктури та боротьби з кіберзлочинністю. Відповідність законодавства європейським стандартам відкриває можливості для співпраці, обміну інформацією та залучення міжнародної допомоги у сфері кіберзахисту.

Однак, незважаючи на позитивні зрушення, правове забезпечення інформаційної безпеки в Україні має низку проблемних моментів. Серед них — надмірна фрагментарність законодавства, відсутність чіткої системності та недостатній рівень узгодженості між окремими нормативними актами. В багатьох випадках закони не містять конкретних механізмів реалізації проголошених положень або залишають їх на розсуд відомчих інструкцій, що створює правову невизначеність.

Аналіз правових аспектів забезпечення інформаційної безпеки в Україні дозволяє виявити певні структурні та практичні проблеми, які істотно знижують ефективність її функціонування. З одного боку, у державі створено низку важливих законів, що регулюють сферу інформаційних відносин, кібербезпеки, захисту персональних даних та державної таємниці. З іншого боку, їхня фрагментарність, недостатня узгодженість і нерідко декларативний характер

багатьох положень свідчать про потребу у комплексному перегляді й модернізації нормативного поля.

Одним із найбільш відчутних недоліків є відсутність системного підходу до законодавчого регулювання. Наявні правові акти часто ухвалювалися як реакція на окремі події чи виклики — масштабні кібератаки, витоки даних або вимоги міжнародних партнерів. В результаті законодавство має розрізнений характер, що ускладнює його практичне застосування і створює ризики дублювання чи суперечності норм. Для прикладу, питання кіберзахисту врегульовано одночасно кількома законами й підзаконними актами, що нерідко призводить до неузгодженості у визначенні повноважень державних органів.

Ще одним суттєвим недоліком є недостатній рівень конкретизації положень багатьох законів. В них часто визначаються лише загальні напрями діяльності або принципи, тоді як механізми реалізації залишаються невизначеними. Це створює ситуацію правової невизначеності, коли практичне застосування норм залежить від відомчих інструкцій, які можуть змінюватися без широкого суспільного обговорення. Така ситуація особливо небезпечна у сфері інформаційної безпеки, де зволікання чи нечіткість у правовому регулюванні можуть призвести до серйозних загроз національній безпеці.

Важливою проблемою є також слабка інтеграція національного законодавства з міжнародними стандартами. Попри проголошений курс на європейську інтеграцію, гармонізація законодавства з правовою базою Європейського Союзу просувається повільно. Це стосується як загальних положень про кібербезпеку, так і спеціальних сфер, зокрема захисту персональних даних. Закон «Про захист персональних даних» формально враховує норми GDPR, однак механізми їхньої реалізації в Україні значно слабші, що обмежує ефективність контролю за обробкою даних громадян і знижує довіру до державних інституцій.

Крім того, у чинному законодавстві недостатньо уваги приділено питанню захисту критичної інформаційної інфраструктури. Хоча окремі положення існують у законі про кібербезпеку, чіткої системи ідентифікації об’єктів

критичної інфраструктури, встановлення стандартів їхнього захисту та відповідальності за їхню безпеку поки що немає. Це створює ризики для енергетичного сектору, фінансової системи, транспортних мереж та інших сфер, які є життєво важливими для функціонування держави.

Серед напрямів удосконалення законодавства можна виділити кілька ключових. По-перше, необхідно забезпечити системність та узгодженість правового регулювання. Це передбачає кодифікацію та уніфікацію нормативних актів, створення єдиного базового закону чи кодексу, що визначав би основи інформаційної безпеки, взаємозв'язок між різними суб'єктами та механізми їхньої взаємодії.

По-друге, важливо підвищити рівень конкретизації норм. Закони мають містити чіткі положення щодо механізмів реалізації, процедур контролю та відповідальності за порушення. Це дозволить уникнути надмірної залежності від підзаконних актів і забезпечить більш прозору та передбачувану систему регулювання.

По-третє, пріоритетним завданням є подальша гармонізація національного законодавства з правом Європейського Союзу. Це стосується не лише сфери персональних даних, але й більш широких аспектів кібербезпеки, включаючи захист критичної інфраструктури, обмін інформацією про кіберінциденти та створення механізмів транскордонної співпраці. Впровадження європейських стандартів не тільки підвищить рівень захищеності держави, а й сприятиме інтеграції України в єдиний європейський цифровий простір.

Удосконалення законодавства у сфері інформаційної безпеки має супроводжуватися посиленням інституційної спроможності органів державної влади. Навіть найкраще сформульовані правові норми залишатимуться малоефективними без належних ресурсів, кваліфікованих кадрів і сучасних технологій, які б дозволяли їх практично реалізовувати.

В цілому, попри наявність основних законодавчих актів, правове поле інформаційної безпеки в Україні потребує глибокої модернізації. Вдосконалення законодавства має бути спрямоване на усунення фрагментарності, підвищення

конкретності норм, інтеграцію з європейськими стандартами та створення ефективних механізмів практичного втілення. Лише у такому разі нормативно-правова база зможе стати дієвим інструментом забезпечення інформаційної безпеки держави й підвищення її стійкості до сучасних викликів.

1.3. Основні загрози та виклики інформаційній безпеці в державному секторі

У сучасному цифровому середовищі інформаційна безпека постає не лише як технічне чи правове завдання, а як комплексна діяльність, спрямована на протидію широкому спектру загроз, що мають різну природу, масштаби та наслідки. Для систематизації цих ризиків важливо застосовувати класифікацію загроз, яка дозволяє структурувати знання про небезпеки, визначати пріоритети захисту та розробляти цілеспрямовані стратегії реагування.

В науковій та практичній літературі існують різні підходи до класифікації загроз інформаційній безпеці. Найпоширенішим є поділ за джерелами походження загроз, що дозволяє виокремити внутрішні та зовнішні фактори ризику. Внутрішні загрози пов’язані з діяльністю співробітників організацій, зокрема їхньою недбалістю, недостатнім рівнем компетентності або навіть умисними діями, спрямованими на завдання шкоди. В державному секторі внутрішні ризики часто виникають через низький рівень культури інформаційної безпеки, неналежне використання інформаційних систем, слабкий контроль за доступом до даних чи витік інформації внаслідок людського фактору. Зовнішні загрози походять від суб’єктів за межами організації та найчастіше пов’язані з кібератаками, зламами інформаційних систем, поширенням шкідливого програмного забезпечення чи діяльністю організованих злочинних угруповань та ворожих держав.

Інший важливий критерій класифікації ґрунтується на характері впливу загроз. В цьому випадку виділяють технічні, організаційні, соціальні та природні фактори. Технічні загрози включають використання уразливостей програмного

забезпечення, хакерські атаки, DDoS-атаки, впровадження вірусів, троянів та іншого шкідливого коду. Організаційні загрози виникають унаслідок недосконалості внутрішніх процедур управління, відсутності належних політик безпеки або їх неналежної реалізації. Соціальні загрози пов’язані з маніпуляціями людьми — наприклад, методами соціальної інженерії, коли зловмисники отримують доступ до конфіденційної інформації через психологічний вплив на працівників. Природні загрози, як-от пожежі, повені чи техногенні аварії, хоча і не є навмисними, проте також здатні знищити або пошкодити інформаційні ресурси державного сектору.

Важливим аспектом класифікації є розподіл загроз за їхніми наслідками. Тут можна виокремити загрози конфіденційності, цілісності та доступності інформації. Загрози конфіденційності стосуються несанкціонованого доступу до даних, що може призвести до витоку державної чи персональної інформації. Порушення цілісності інформації означає її спотворення або знищення, що робить дані непридатними для використання у процесах прийняття рішень. Загрози доступності пов’язані з блокуванням чи перериванням роботи інформаційних систем, що може паралізувати діяльність державних органів, особливо у кризових ситуаціях.

Крім того, загрози можна класифікувати за рівнем організованості та масштабом дії. Існують індивідуальні атаки, які здійснюють окремі зловмисники, та організовані кампанії, що координуються злочинними угрупованнями або навіть державними структурами. За масштабом впливу загрози можуть бути локальними, коли вони стосуються конкретної установи чи органу, або глобальними, коли наслідки поширюються на цілі галузі, регіони чи навіть державу в цілому. Прикладом останніх є масові кібератаки на об’єкти критичної інфраструктури, які можуть викликати серйозні соціально-економічні потрясіння.

Окрему групу становлять гібридні загрози, характерні для сучасних воєнних і політичних конфліктів. Вони поєднують у собі кібернетичні атаки, інформаційно-психологічний вплив, дезінформацію та пропаганду. Для України

цей аспект має особливе значення у контексті протидії зовнішній агресії, коли інформаційний простір стає не менш важливим полем боротьби, ніж традиційні військові дії.

Різноманітність і багатовимірність загроз інформаційній безпеці особливо виразно проявляється у сфері кіберзлочинності, яка вже давно перестала бути проблемою лише комерційних структур чи приватних користувачів. Сучасні державні установи є одними з головних мішеней для кібератак, адже вони зосереджують у собі значні обсяги чутливої інформації, управляють стратегічно важливими процесами та відповідають за функціонування критичної інфраструктури. Саме тому кіберзлочинність стала не лише кримінальною категорією, а й одним із найнебезпечніших інструментів впливу на політичну стабільність, національну безпеку й міжнародні відносини.

Кіберзлочинність у контексті державного сектору охоплює широкий спектр протиправної діяльності. До неї відносять злам державних інформаційних систем з метою викрадення чи знищення даних, поширення шкідливого програмного забезпечення, блокування роботи серверів і порталів електронного урядування, а також атаки на інформаційні системи критичних об’єктів, таких як енергетичні підприємства чи банківська інфраструктура. Особливо небезпечними є атаки типу ransomware, коли державні бази даних шифруються, а зловмисники вимагають викуп за їх відновлення. Такі випадки не лише підривають довіру до державних інституцій, але й паралізують їхню діяльність у критичні моменти.

Державні установи стають мішенями хакерів і через стратегічне значення інформації, якою вони володіють. Це можуть бути персональні дані громадян, конфіденційні відомості про роботу урядових структур, дипломатичні документи чи матеріали оборонного характеру. Викрадення або оприлюднення такої інформації має подвійний ефект: з одного боку, створює безпосередні загрози для національної безпеки, а з іншого — може використовуватися як інструмент політичного тиску чи дестабілізації.

Особливістю сучасних хакерських атак є їхня організованість і високий рівень технічної складності. Багато з них здійснюються не окремими кіберзлочинцями, а спеціалізованими угрупованнями, які мають значні ресурси та нерідко діють у координації з державними структурами іноземних держав. Такі атаки носять характер кібершпигунства або навіть кібертероризму, адже їхньою метою є не лише отримання фінансової вигоди, а й підрив політичної та економічної стабільності.

Україна як держава, що перебуває у стані збройної агресії, особливо гостро відчуває загрозу від кібератак. Яскравим прикладом стали події 2015–2016 років, коли хакерські атаки на енергетичні компанії призвели до масових відключень електроенергії. Інший відомий випадок — поширення вірусу Petya/NotPetya у 2017 році, який паралізував роботу державних органів, банків, транспортних підприємств та комерційних структур, завдавши мільярдних збитків. Ці приклади показали, що кібератаки здатні не лише шкодити інформаційним системам, але й мати катастрофічні соціально-економічні наслідки.

Важливо зазначити, що характер сучасних атак значно ускладнює їхнє виявлення й нейтралізацію. Хакери застосовують багаторівневі методи маскування, використовують тактики фішингу, соціальної інженерії, багатовекторні атаки. Часто вони діють непомітно протягом тривалого часу, збираючи дані чи поступово отримуючи контроль над ключовими системами. Така прихована діяльність, яку називають APT-атаками (Advanced Persistent Threats), є особливо небезпечною для державних установ, адже дозволяє зловмисникам отримувати довгостроковий доступ до критично важливої інформації.

Проблема кіберзлочинності загострюється ще й тим, що державний сектор часто має обмежені ресурси для захисту. Застаріле обладнання, недостатня кількість кваліфікованих кадрів, нерівномірний рівень цифрової грамотності працівників створюють сприятливі умови для реалізації атак. Крім того, слабкою ланкою часто стає відсутність належної координації між різними державними

органами у сфері кіберзахисту, що унеможливлює своєчасний обмін інформацією про інциденти та швидке реагування на загрози.

Також, не можна оминути увагою менш очевидний, але не менш небезпечний пласт загроз — ті, що виникають усередині самих державних структур. Зовнішній тиск у формі кібератак часто доповнюється або навіть посилюється внутрішніми ризиками, які пов’язані з низьким рівнем інформаційної культури, недотриманням правил безпеки та людським фактором. Саме внутрішні слабкості нерідко стають причиною успішності зовнішніх атак, оскільки навіть найсучасніші технічні системи захисту не здатні повністю компенсувати помилки персоналу чи недоліки в організації роботи.

Під внутрішніми ризиками в інформаційній безпеці розуміють насамперед недобросовісні або необережні дії співробітників, а також організаційні прогалини, що створюють вразливості в захищеності інформаційних систем. Найчастіше такі ризики проявляються у вигляді ненавмисних порушень — наприклад, використання працівниками слабких паролів, відкриття підозрілих електронних листів, неконтрольоване копіювання документів чи завантаження даних на незахищені носії. У результаті навіть звичайна необачність може стати «точкою входу» для кіберзлочинців.

Водночас не варто ігнорувати й умисні дії внутрішніх користувачів. Працівники, які мають доступ до конфіденційних даних, можуть навмисно поширювати їх чи використовувати для особистої вигоди. Такі випадки інсайдерських загроз становлять серйозну проблему, оскільки виявити їх значно складніше, ніж зовнішні атаки. Додатковим фактором ризику стає корупційна складова, коли доступ до інформації використовується як інструмент тиску, маніпуляцій або незаконного збагачення.

Ключовим чинником, що поглиблює внутрішні ризики, є недостатньо сформована інформаційна культура у державному секторі. Багато працівників державних органів не сприймають питання інформаційної безпеки як невід’ємну складову своєї щоденної діяльності. Часто безпека розглядається як технічна сфера, що перебуває у компетенції виключно IT-відділів чи спеціалізованих

підрозділів. У такій ситуації правила захисту інформації не стають частиною організаційної культури, а залишаються формальними вимогами, які ігноруються в умовах високого навантаження чи нестачі часу.

Серйозною проблемою є й низький рівень цифрової грамотності значної частини державних службовців. В умовах швидкого розвитку інформаційних технологій багато співробітників виявляються неготовими адекватно реагувати на нові виклики: вони не розрізняють фішингові повідомлення, не усвідомлюють важливості багатофакторної автентифікації, не знають, як правильно поводитися з електронними носіями даних. Усе це значно підвищує вразливість інформаційних систем держави.

Важливим елементом внутрішніх ризиків є також недоліки в організації управління інформаційною безпекою. Нерідко відсутні чіткі протоколи реагування на інциденти, не проводяться регулярні аудити інформаційних систем, а заходи з навчання персоналу носять епізодичний і формальний характер. В результаті навіть при наявності певних засобів захисту вони не дають належного ефекту через слабкий рівень їхньої інтеграції в управлінські процеси.

Отже, внутрішні ризики та проблеми інформаційної культури формують критичний пласт загроз, що доповнює і підсилює зовнішні виклики. Їхня небезпека полягає в тому, що вони часто залишаються непоміченими, доки не призводять до серйозних наслідків — витоків даних, зривів у роботі державних систем чи компрометації управлінських рішень. Для ефективного протистояння цим загрозам необхідно формувати комплексний підхід, що передбачає не лише технічні засоби захисту, але й розвиток інформаційної культури, підвищення рівня цифрової грамотності, створення атмосфери персональної відповідальності кожного співробітника за безпеку інформаційного середовища держави.

РОЗДІЛ 2. СИСТЕМИ ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДЕРЖАВНОМУ СЕКТОРІ

2.1. Організаційно-правові механізми захисту інформації

Організаційно-правові механізми забезпечення інформаційної безпеки в державному секторі передбачають й створення цілісної системи інституцій, які координують, контролюють і реалізують політику у цій сфері. Іншими словами, без належним чином організованої інституційної архітектури державна політика в галузі інформаційної безпеки залишатиметься декларативною і не матиме реального впливу на захист національних інтересів.

У сучасних умовах в Україні сформовано багаторівневу систему органів, відповідальних за інформаційну безпеку, яка охоплює як стратегічний, так і операційно-тактичний рівні. Центральним координуючим суб'єктом у цій системі виступає Рада національної безпеки і оборони України (РНБО), що визначає ключові пріоритети, затверджує стратегії, а також контролює виконання заходів у сфері національної безпеки, включно з інформаційною. РНБО забезпечує міжвідомчу координацію, інтегруючи діяльність усіх інших державних структур, та виконує функцію стратегічного центру ухвалення рішень.

Важливу роль відіграє Служба безпеки України (СБУ), яка відповідає за контррозвідувальну діяльність у сфері захисту інформаційного простору. Її компетенція включає виявлення та протидію кіберзагрозам, запобігання інформаційним диверсіям, боротьбу з дезінформацією та інформаційним тероризмом. У структурі СБУ функціонують спеціалізовані підрозділи, які займаються кібербезпекою та кіберзахистом державних органів і критичної інфраструктури.

Важливим елементом організаційної системи є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Цей орган виконує

функції у сфері технічного та криптографічного захисту інформації, забезпечує функціонування урядового зв'язку, сертифікує системи захисту даних, а також координує роботу з питань захисту інформації в державних установах. Саме ДССЗЗІ відповідає за розробку державних стандартів криптографічного захисту та впровадження механізмів електронної ідентифікації.

Окреме місце у системі займає Кіберполіція України, яка є підрозділом Національної поліції. Її діяльність спрямована на виявлення, розслідування та попередження кіберзлочинів, зокрема атак на державні органи. Кіберполіція забезпечує взаємодію із зарубіжними правоохоронними структурами, бере участь у міжнародних операціях із боротьби з кіберзлочинністю, а також здійснює інформаційно-просвітницьку роботу серед громадян і організацій щодо правил кібергігієни.

Не менш важливу роль відіграє й Міністерство цифрової трансформації України, яке відповідає за розвиток електронного урядування, цифрових сервісів та впровадження сучасних інформаційних технологій у діяльність держави. Хоча цей орган безпосередньо не є силовою структурою, він опосередковано впливає на інформаційну безпеку, адже визначає правила функціонування електронної інфраструктури та відповідає за її модернізацію. У компетенції Мінцифри, теж, перебуває популяризація цифрової грамотності, що є складовою формування культури інформаційної безпеки.

Значний внесок у формування політики здійснюють також Міністерство оборони України та Генеральний штаб Збройних Сил України, які відповідають за кібероборону та захист інформаційних систем у військовій сфері. В умовах війни зростає значення спеціалізованих військових підрозділів, що забезпечують кіберзахист оборонних систем, здійснюють кіберрозвідку та протидіють інформаційним диверсіям з боку агресора.

Важливо підкреслити, що організаційна система захисту інформації в Україні не обмежується лише державними структурами. В ній активно задіяні наукові установи, освітні заклади, а також громадські організації, які беруть участь у розробці концепцій інформаційної безпеки, підготовці фахівців та

моніторингу стану інформаційного простору. Проте, якраз державні органи залишаються базовим фундаментом, що визначає пріоритети, формує законодавчі ініціативи та здійснює практичні заходи із забезпечення безпеки в інформаційній сфері.

Водночас, ефективність роботи такої системи значною мірою залежить від того, як безпекові підходи трансформуються на рівень окремих державних установ. Саме там, у щоденній діяльності органів влади, відбувається практичне втілення загальнодержавної політики в конкретні правила, процедури й стандарти, які мають забезпечувати захист інформаційних ресурсів.

Політика інформаційної безпеки в державних органах являє собою систему внутрішніх норм, інструкцій та регламентів, які визначають порядок роботи з інформацією, правила доступу до неї, засоби захисту, відповідальність персоналу за порушення вимог безпеки. Вона формується на основі національного законодавства, міжнародних стандартів (ISO/IEC 27001, ISO/IEC 27002 тощо) та методичних рекомендацій спеціалізованих органів, зокрема Державної служби спеціального зв'язку та захисту інформації України. Завдяки цьому політика інформаційної безпеки стає практичним інструментом, що забезпечує реалізацію вимог законодавства у конкретній установі.

Серед ключових компонентів такої політики варто виокремити чітке визначення ролей і відповідальності співробітників у сфері інформаційної безпеки. У багатьох установах створюються спеціалізовані підрозділи або визначаються відповідальні особи, які здійснюють координацію захисних заходів, контролюють виконання внутрішніх регламентів та взаємодіють із національними органами у разі кіберінцидентів. Важливо, щоб політика охоплювала не лише IT-відділи, але й усіх співробітників, адже інформаційна безпека напряму залежить від рівня дисципліни та свідомості кожного працівника.

Особливу увагу політика інформаційної безпеки приділяє питанням управління доступом до інформаційних систем. Йдеться про впровадження механізмів автентифікації користувачів, використання багатофакторного

захисту, обмеження прав доступу відповідно до службових обов’язків, а також постійний моніторинг дій користувачів у системі. Завдяки цьому мінімізується ризик несанкціонованого доступу до чутливих даних як з боку зовнішніх, так і з боку внутрішніх суб’єктів.

Ще одним важливим напрямом є регулювання обробки та зберігання інформації. Політика має визначати правила роботи з персональними даними, порядок їхнього захисту, умови передачі третім сторонам, використання шифрування для захисту інформаційних потоків. У сучасних умовах, коли державні установи все активніше переходять на електронні документообіг і цифрові сервіси, забезпечення безпеки даних стає критичною передумовою функціонування таких систем.

Важливо, що політика інформаційної безпеки також включає процедури реагування на інциденти. Це означає наявність чіткого алгоритму дій у разі виявлення витоку даних, спроби кібератаки чи порушення роботи інформаційної системи. Такий алгоритм передбачає повідомлення відповідальних осіб, локалізацію загрози, фіксацію інциденту, взаємодію з уповноваженими державними органами, а також аналіз причин і наслідків для недопущення повторення подібних випадків у майбутньому.

Окремим напрямом реалізації політики є навчання та підвищення рівня інформаційної культури співробітників. Регулярні тренінги, інструктажі та тестування знань із питань кібергігієни дозволяють знизити ризик внутрішніх загроз, спричинених людським фактором. Формування середовища, у якому дотримання правил інформаційної безпеки стає органічною частиною робочих процесів, має стратегічне значення для стійкості державних установ.

Але, рзробка внутрішніх політик інформаційної безпеки в державних установах неможлива без опори на загальноприйняті правила та методології, які виходять за межі національного законодавства. Для того щоб внутрішні регламенти були ефективними й водночас узгодженими з глобальними практиками, вони повинні ґрунтуватися на міжнародних стандартах, що задають уніфіковані вимоги до організації систем управління інформаційною безпекою.

Стандарти міжнародного рівня дозволяють забезпечити сумісність підходів, створити єдину термінологічну та методологічну основу і підвищити ефективність протидії загрозам, які часто мають транснаціональний характер.

Міжнародні стандарти у сфері інформаційної безпеки виконують кілька важливих функцій. По-перше, вони встановлюють чіткі орієнтири для розробки систем управління інформаційною безпекою (СУІБ), які можуть застосовуватися як у приватному секторі, так і в державному управлінні. По-друге, вони створюють основу для оцінки рівня зрілості інформаційної безпеки конкретної установи, що дозволяє виявити слабкі місця та запровадити заходи для їхнього усунення. По-третє, вони забезпечують міжнародну співставність практик, завдяки чому державні органи можуть інтегруватися в глобальну систему кіберзахисту та ефективно співпрацювати з іншими країнами.

Серед найбільш відомих і поширених стандартів слід виокремити ISO/IEC 27001, який визначає вимоги до створення, впровадження та постійного вдосконалення систем управління інформаційною безпекою. Він передбачає комплексний підхід, що охоплює організаційні, технічні та кадрові аспекти безпеки. У контексті державного сектору цей стандарт є особливо цінним, адже він дозволяє створювати системи захисту, що поєднують стратегічні цілі державної політики з операційними завданнями конкретних установ.

Не менш важливим є стандарт ISO/IEC 27002, який надає рекомендації щодо практичного впровадження заходів захисту. У ньому окреслюються політики управління доступом, захисту даних, криптографічних методів, а також управління інцидентами інформаційної безпеки. Використання цього стандарту в державних установах сприяє уніфікації підходів, що дозволяє органам влади говорити «однією мовою» в питаннях кіберзахисту та обміну інформацією.

Варто зазначити й про стандарти Міжнародного союзу електрозв’язку (ITU) та рекомендації Європейського агентства з мережевої та інформаційної безпеки (ENISA). Вони розробляють рамкові документи, що допомагають країнам вибудовувати власні стратегії інформаційної безпеки відповідно до світових тенденцій. Для України, яка інтегрується в європейський правовий

простір, такі стандарти є не лише орієнтиром, але й необхідною умовою гармонізації законодавства з нормами Європейського Союзу.

Застосування міжнародних стандартів має ще один важливий аспект — підвищення довіри громадян і міжнародних партнерів до державних цифрових сервісів. Коли державні установи декларують і доводять відповідність своїх систем безпеки загальноприйнятим міжнародним вимогам, це формує позитивний імідж держави як надійного партнера у сфері цифрової взаємодії. Особливо це актуально у сфері захисту персональних даних, де відповідність європейському Регламенту GDPR є ключовою умовою міжнародної співпраці.

Важливо підкреслити, що міжнародні стандарти не є статичними документами. Вони регулярно оновлюються відповідно до нових викликів і загроз, що з’являються у цифровому середовищі. Це дозволяє державним установам, які орієнтуються на ці стандарти, залишатися гнучкими й адаптивними до змін, своєчасно впроваджуючи нові механізми захисту. Тому, дотримання міжнародних стандартів у сфері інформаційної безпеки є не лише питанням технічної відповідності, але й стратегічною умовою сталого розвитку та інтеграції у глобальну інформаційну спільноту.

Отже, міжнародні стандарти відіграють фундаментальну роль у формуванні політики та практики інформаційної безпеки в державному секторі. Вони слугують орієнтирами для побудови ефективних систем захисту, забезпечують порівнянність і сумісність підходів на міжнародному рівні, формують основу для довіри громадян і партнерів, а також дозволяють державі оперативно реагувати на нові виклики інформаційної епохи.

2.2. Технологічні рішення для забезпечення інформаційної безпеки

Технологічний вимір інформаційної безпеки є дуже важливим, оскільки саме технічні засоби забезпечують практичну реалізацію політик і принципів, визначених у нормативно-правових та організаційних документах. Одним із найефективніших і найпоширеніших інструментів у цій сфері виступають

криптографічні методи захисту інформації. Вони дозволяють гарантувати конфіденційність, цілісність та автентичність даних, які циркулюють у державних інформаційних системах, а також забезпечують неможливість несанкціонованого доступу до критично важливих відомостей.

Криптографія історично розвивалася як наука про шифрування повідомлень, проте сучасний її зміст набагато ширший. Вона охоплює створення та застосування алгоритмів, що перетворюють інформацію у форму, недоступну для сторонніх осіб без відповідних ключів, а також забезпечують перевірку достовірності джерела та незмінності переданих даних. Для державного сектору це особливо важливо, адже інформаційні ресурси органів влади включають як персональні дані громадян, так і документи стратегічного чи оборонного значення, витік яких може становити загрозу національній безпеці.

У практиці сучасних державних установ використовуються різні види криптографічних засобів, серед яких можна виокремити симетричні та асиметричні алгоритми. Симетричні методи передбачають застосування одного ключа як для шифрування, так і для розшифрування даних. Вони відзначаються високою швидкістю обробки інформації, що робить їх зручними для захисту великих обсягів даних у внутрішніх інформаційних системах. Прикладами таких алгоритмів є AES (Advanced Encryption Standard) та ГОСТ 28147-89, які широко застосовуються як у комерційному секторі, так і в державних структурах.

Асиметричні алгоритми, на відміну від симетричних, використовують два ключі — відкритий і закритий. Цей підхід забезпечує більш високий рівень безпеки, оскільки відкритий ключ може передаватися по незахищених каналах, тоді як приватний залишається у власника. Найвідомішим прикладом такого підходу є алгоритм RSA, а також сучасні методи, що базуються на еліптичних кривих. Для державного сектору особливе значення має використання асиметричної криптографії у створенні електронних цифрових підписів, що гарантують автентичність електронних документів і унеможливлюють їх підробку.

Важливим елементом криптографічного захисту є застосування електронного цифрового підпису (ЕЦП). Він дозволяє не лише підтверджувати достовірність документів, але й забезпечує юридичну значимість електронного документообігу. У державному секторі України функціонування системи ЕЦП регламентується відповідними нормативно-правовими актами, а ключовим оператором є Центральний засвідчувальний орган. Використання ЕЦП є фундаментом для впровадження електронного урядування, електронних сервісів для громадян та бізнесу, що в свою чергу підвищує прозорість і ефективність державного управління.

Ще однією важливою сферою застосування криптографії є захист каналів зв'язку. Використання протоколів SSL/TLS, VPN-технологій та інших криптографічних рішень забезпечує безпечну передачу даних між державними органами, а також захист від перехоплення та підміни інформації під час її транспортування мережею. Це особливо важливо в умовах постійних кібератак, які спрямовані на втручання в інформаційні ресурси органів влади.

В сучасних умовах криптографія набуває особливого значення й у сфері хмарних технологій, якими починають користуватися державні установи для зберігання даних і надання електронних послуг. Використання криптографічних методів дозволяє гарантувати, що навіть у випадку витоку даних з хмарного сховища вони залишаться недоступними для зловмисників.

Водночас, застосування криптографічного захисту не є універсальним рішенням усіх проблем інформаційної безпеки. Його ефективність залежить від правильної організації процесів управління ключами, суворого дотримання процедур автентифікації та контролю доступу, а також від наявності нормативного забезпечення, яке регламентує порядок використання криптографічних засобів у державному секторі. Варто зазначити, що у випадку неякісної реалізації алгоритмів чи неправильної експлуатації навіть найсучасніші криптографічні системи можуть виявитися вразливими.

Криптографічний захист не може повною мірою гарантувати безпеку інформаційних систем без чітко організованого механізму контролю за тим, хто

саме отримує доступ до цих даних і яким чином цей доступ реалізується. Тому ключовим доповненням до криптографічних методів виступають системи контролю доступу та аутентифікації, які визначають межі використання інформаційних ресурсів та регламентують права користувачів у державних установах.

Контроль доступу — це сукупність організаційних і технічних заходів, спрямованих на обмеження можливостей взаємодії з інформаційними ресурсами відповідно до визначених правил. Він базується на принципі мінімальних привілеїв, за яким кожен користувач отримує лише ті права, що необхідні для виконання його службових обов’язків. В державному секторі цей принцип має критичне значення, адже надмірні повноваження користувачів можуть призвести до витоків службової або секретної інформації, навіть якщо ці витоки не є наслідком зловмисних дій, а виникають через необережність чи недотримання правил безпеки.

Аутентифікація у свою чергу є процесом перевірки автентичності користувача, що звертається до інформаційної системи. Вона покликана підтвердити, що суб’єкт, який намагається отримати доступ, дійсно є тим, за кого себе видає. У державних інформаційних системах застосовуються різні методи аутентифікації, які можна поділити на кілька основних груп: аутентифікація на основі знання (наприклад, паролі або PIN-коди), на основі володіння (смарт-карти, токени, електронні ключі) та на основі біометричних характеристик (відбитки пальців, розпізнавання обличчя, голосу тощо).

Окремої уваги заслуговує багатофакторна аутентифікація, яка поєднує два чи більше методи перевірки особи. Для державного сектору такий підхід є особливо актуальним, адже дозволяє значно знизити ризик несанкціонованого доступу навіть у випадках компрометації одного з факторів, наприклад, викрадення пароля. Сучасні тенденції вказують на необхідність впровадження багатофакторної аутентифікації у всіх критично важливих державних інформаційних системах, зокрема в системах електронного документообігу,

банківських і фінансових ресурсах органів влади, а також у сервісах електронного урядування.

Не менш важливим аспектом є побудова ієрархічних систем розмежування доступу. В державних структурах інформація часто має різний рівень важливості — від відкритої до такої, що становить державну таємницю. Тому застосування диференційованого доступу, який передбачає чітке зонування прав користувачів, дозволяє мінімізувати ймовірність несанкціонованого ознайомлення із критичними даними. При цьому контроль доступу може бути реалізований як на рівні операційних систем і програмного забезпечення, так і на рівні фізичної інфраструктури, де застосовуються карткові системи, біометричні сканери та інші технічні засоби.

Особливу роль у системах контролю доступу відіграє аудит і протоколювання дій користувачів. Це дозволяє не лише своєчасно виявляти спроби несанкціонованого доступу, але й відслідковувати поведінку співробітників у межах їхніх повноважень. Наявність журналів подій створює можливості для ретроспективного аналізу інцидентів та допомагає підвищити прозорість функціонування інформаційних систем.

Варто зауважити, що впровадження систем контролю доступу та аутентифікації в державному секторі тісно пов’язане з питанням довіри суспільства до державних цифрових послуг. Громадяни повинні бути впевнені, що їхні персональні дані захищені і що доступ до них можуть отримати лише уповноважені особи. Саме тому розвиток таких систем є важливим елементом цифрової трансформації держави, спрямованої на побудову ефективного, безпечного та прозорого електронного врядування.

В цілому, налагоджені системи контролю доступу та аутентифікації значно підвищують рівень захищеності державних інформаційних ресурсів, але, навіть, вони не здатні повністю усунути всі ризики. Зловмисники постійно вдосконалюють свої методи, використовуючи складніші інструменти атак, автоматизовані бот-мережі та соціотехнічні прийоми, що обходять класичні механізми захисту. В такій динамічній ситуації традиційні підходи виявляються

недостатньо ефективними, і на перший план виходить застосування новітніх технологій, серед яких особливе місце займають системи на основі штучного інтелекту.

Штучний інтелект у сфері інформаційної безпеки передбачає використання алгоритмів машинного навчання, нейронних мереж та інших методів обробки даних для автоматизованого виявлення аномалій, прогнозування атак і оперативного реагування на інциденти. Основна перевага таких систем полягає у здатності аналізувати великі обсяги інформації в режимі реального часу та знаходити закономірності, які неможливо виявити традиційними методами чи навіть людськими аналітиками. Для державного сектору, де йдеться про захист критичної інфраструктури та персональних даних мільйонів громадян, це відкриває принципово нові можливості підвищення рівня кіберзахисту.

Одним із ключових напрямів використання штучного інтелекту є системи виявлення аномалій. Вони будуються на аналізі «нормальної» поведінки користувачів і систем, після чого будь-які відхилення від цієї поведінки автоматично позначаються як потенційні загрози. Такий підхід дозволяє своєчасно виявляти навіть ті атаки, які не мають чітко визначених сигнатур у базах даних, тобто є новими або модифікованими. Це особливо актуально для державних органів, які часто стають мішенню цілеспрямованих і нетипових атак.

Ще одним важливим аспектом є автоматизація процесів реагування на інциденти. Алгоритми штучного інтелекту здатні не лише виявляти загрози, але й пропонувати оптимальні дії для їх нейтралізації або навіть самостійно здійснювати блокування підозрілих дій. Це значно скорочує час реагування, що критично важливо у випадках, коли рахунок іде на хвилини, а від швидкості прийняття рішень залежить цілісність державних інформаційних систем.

Не менш перспективним напрямом є використання штучного інтелекту для прогнозування кіберзагроз. На основі аналізу історичних даних, моделей поведінки зловмисників і тенденцій у кіберпросторі такі системи здатні передбачати потенційні атаки ще до того, як вони відбудуться. Для державного

управління це означає можливість переходу від реактивної до проактивної моделі захисту, коли небезпека нейтралізується ще на етапі планування атаки.

Окремо слід відзначити роль штучного інтелекту у сфері розпізнавання соціотехнічних атак, зокрема фішингу чи спроб маніпуляцій через електронну пошту та соціальні мережі. Сучасні алгоритми здатні аналізувати стиль написання повідомлень, структуру тексту, використання підозрілих посилань чи вкладень, автоматично виявляючи потенційно небезпечні комунікації. Це суттєво підвищує рівень інформаційної культури в державних установах, адже навіть добре навчені працівники інколи можуть стати жертвами таких атак.

Важливо підкреслити, що впровадження систем штучного інтелекту у сфері кібербезпеки потребує належної організації, зокрема якісних і об'ємних наборів даних для навчання моделей, постійного оновлення алгоритмів, а також контролю з боку фахівців. Інакше існує ризик появи хибнопозитивних спрацьовувань, які можуть дестабілізувати роботу державних установ, або навпаки — пропуску реальних атак через недосконалість моделей.

Загалом, використання штучного інтелекту у сфері інформаційної безпеки державного сектору є одним із найбільш перспективних напрямів розвитку сучасних технологічних рішень. Воно дозволяє не лише підвищити ефективність виявлення і реагування на загрози, але й закладає основу для формування адаптивних систем кіберзахисту, здатних самостійно навчатися і вдосконалюватися. В результаті державні органи отримують унікальний інструмент, що забезпечує стійкість інформаційної інфраструктури в умовах постійно зростаючих і змінних викликів цифрової епохи.

2.3. Стратегії кіберзахисту державного сектору

Надійна оборона інформаційного простору передбачає створення комплексної, багаторівневої та інтегрованої системи, яка б охоплювала всі рівні державного управління, приватний сектор і суспільство загалом. Побудова національної системи кібербезпеки є ключовою умовою ефективного

функціонування держави в умовах цифрової трансформації та зростаючої кількості кіберзагроз.

Національна система кібербезпеки — це сукупність інституційних, нормативних, організаційних і технічних механізмів, які забезпечують захист критичної інформаційної інфраструктури, державних інформаційних ресурсів, персональних даних громадян і цифрових сервісів від кібератак, несанкціонованого доступу чи інформаційних диверсій. Її побудова повинна ґрунтуватися на чітких принципах: централізації стратегічного управління, розподілу відповідальності між органами влади, прозорої взаємодії з приватним сектором і дотримання міжнародних стандартів у сфері інформаційної безпеки.

Ключовим елементом такої системи виступає державна координаційна інституція, яка відповідає за формування політики та координацію дій у сфері кібербезпеки. В багатьох країнах цю роль виконують спеціальні національні центри або агентства, що діють як головний орган, відповідальний за виявлення, аналіз і реагування на кібератаки. В Україні подібну функцію виконує Державна служба спеціального зв’язку та захисту інформації, яка разом із Службою безпеки України, Міністерством оборони та іншими структурами формує єдиний фронт кібероборони.

Невід’ємною складовою є нормативно-правове забезпечення, яке встановлює загальні правила функціонування кіберпростору. Йдеться про закони, підзаконні акти та державні стандарти, що регламентують обов’язки суб’єктів критичної інфраструктури, порядок реагування на інциденти, обмін інформацією між органами влади та приватними компаніями. Особливу роль тут відіграє Закон України «Про основні засади забезпечення кібербезпеки України», який заклав фундамент для створення єдиної системи кіберзахисту.

Важливим напрямом є захист критичної інформаційної інфраструктури, що включає енергетику, транспорт, банківсько-фінансову систему, медицину, державні інформаційні реєстри тощо. Побудова національної системи кібербезпеки передбачає створення механізмів моніторингу та швидкого реагування на загрози, які можуть паралізувати діяльність цих секторів. В цьому

контексті необхідною є тісна співпраця держави з приватними компаніями, адже значна частина критичної інфраструктури перебуває у їхньому володінні.

Не менш суттєвим елементом є кадрове забезпечення та розвиток компетенцій. Жодна, навіть найсучасніша система, не буде ефективною без висококваліфікованих спеціалістів, здатних оперативно реагувати на інциденти. Тому у рамках національної стратегії кіберзахисту важливо розвивати освітні програми, підвищення кваліфікації кадрів у сфері кібербезпеки, а також стимулювати створення науково-дослідних центрів, які б займалися інноваційними розробками.

Сучасні національні системи кібербезпеки спираються й на використання інноваційних технологій, зокрема штучного інтелекту, автоматизованих систем моніторингу, блокчейн-рішень та інструментів прогнозування загроз. Вони дозволяють державі не лише реагувати на вже здійснені атаки, але й запобігати їм на ранніх етапах.

Варто підкреслити й міжнародний вимір побудови національної системи кібербезпеки. Україна, як держава, що активно інтегрується у європейський і світовий політичний простір, має узгоджувати свою стратегію з євроатлантичними стандартами. Участь у глобальних ініціативах, співпраця з НАТО, Європейським Союзом і спеціалізованими міжнародними організаціями дозволяє обмінюватися інформацією про загрози, підвищувати рівень готовності та впроваджувати найкращі практики.

Проте, навіть найкраще вибудувана система не може гарантувати повної відсутності атак чи технічних збоїв. В цифровому середовищі завжди залишається ймовірність проникнення зловмисників, витоку даних або порушення функціонування критичних сервісів. Тому, важливим елементом загальної стратегії кіберзахисту є розробка й впровадження спеціалізованих програм реагування на кіберінциденти, які дозволяють не лише швидко локалізувати загрози, а й мінімізувати їхні наслідки та запобігати повторенню у майбутньому.

Програми реагування на кіберінциденти являють собою комплекс організаційних, технічних та процедурних заходів, спрямованих на виявлення, аналіз, нейтралізацію та документування інцидентів інформаційної безпеки. Їхня головна мета — не допустити ескалації загрози та забезпечити безперервність функціонування інформаційних систем, від яких залежать державні послуги, робота установ і довіра громадян. В державному секторі така діяльність є критично важливою, адже збої можуть мати не лише економічні, а й політичні та соціальні наслідки.

Зміст програм реагування зазвичай охоплює кілька ключових етапів. Перший — ідентифікація інциденту, коли спеціалізовані системи моніторингу або аналітики виявляють підозрілу активність. Для цього використовуються як класичні інструменти аналізу журналів подій, так і сучасні рішення на основі штучного інтелекту, здатні фіксувати аномалії у поведінці користувачів чи програм. Другий етап — оцінка масштабу та класифікація інциденту, що дозволяє визначити його критичність і пріоритетність реагування. Це надзвичайно важливо в умовах державних органів, де кожна хвилина затримки може призвести до витоку секретних даних чи зупинки важливих сервісів.

Наступним етапом є локалізація загрози та її нейтралізація. Тут застосовуються різноманітні заходи: від блокування користувацьких облікових записів і відключення заражених сегментів мережі до оперативного застосування оновлень безпеки чи відновлення роботи серверів із резервних копій. В рамках державного сектору ця діяльність часто координується спеціалізованими центрами реагування на комп’ютерні інциденти — CERT (Computer Emergency Response Team) або CSIRT (Computer Security Incident Response Team), які функціонують як на національному, так і на відомчому рівні.

Особливе значення мають програми навчання та симуляційні вправи, які інтегруються у стратегії реагування. Вони передбачають моделювання реальних сценаріїв атак, зокрема масових DDoS-атак, спроб фішингу, шкідливих програм або внутрішніх витоків. Такі тренування допомагають співробітникам державних установ не лише закріплювати теоретичні знання, а й

відпрацьовувати практичні дії у стресових умовах. Для прикладу, в Україні та країнах Європейського Союзу регулярно проводяться міжнародні кібернавчання типу Cyber Europe або Locked Shields, які дозволяють перевірити готовність державних структур до реальних кібератак.

Важливою складовою програм реагування є також система комунікації та інформування. У випадку масштабного інциденту критично необхідно забезпечити швидкий обмін інформацією між усіма дотичними структурами — державними органами, приватними компаніями, міжнародними партнерами. Від ефективності комунікації залежить здатність оперативно обмежити наслідки та запобігти поширенню атаки.

Не слід забувати й про аналіз після інциденту (post-incident review), який передбачає ретельне вивчення причин події, її перебігу та ефективності застосованих заходів реагування. На основі таких звітів формуються рекомендації щодо вдосконалення внутрішніх процесів, модернізації технічних засобів та підвищення кваліфікації персоналу. Це створює замкнений цикл постійного вдосконалення системи кіберзахисту.

Варто зауважити, що ефективність програм реагування на кіберінциденти багато в чому визначається здатністю державних структур не лише усувати вже наявні загрози, а й передбачати їх виникнення. Лише тоді, коли система кіберзахисту поєднує механізми швидкого реагування з превентивними підходами, можна говорити про справжню стійкість державного сектору до кібератак. Якраз тут на перший план виходять запобіжні заходи та політики ризик-менеджменту, які формують основу для мінімізації вразливостей ще до того, як ними скористаються зловмисники.

Ризик-менеджмент у сфері інформаційної безпеки являє собою комплексну діяльність із виявлення, оцінки та контролю ризиків, пов’язаних із використанням інформаційних систем, технологій і цифрових ресурсів. В державному секторі він охоплює як технічні аспекти (уразливості програмного забезпечення, конфігураційні помилки, неналежний захист каналів зв’язку), так і організаційні (недостатня кваліфікація персоналу, відсутність належних

процедур доступу до інформації, низький рівень культури безпеки). Завдяки системному підходу ризик-менеджмент дозволяє визначити критичні точки, які потребують першочергової уваги, та оптимально розподіляти ресурси на їх усунення.

Одним із ключових елементів у цій сфері є запобіжні заходи, спрямовані на недопущення виникнення інцидентів. До таких належать регулярне оновлення програмного забезпечення та операційних систем, багаторівневий контроль доступу, застосування сучасних методів шифрування, резервне копіювання даних, сегментація мереж і проведення аудитів безпеки. Ці дії створюють базову лінію захисту, яка зменшує ймовірність успішної атаки навіть у разі спроби проникнення.

Не менш важливою складовою є формування політик ризик-менеджменту. Йдеться про розробку і впровадження внутрішніх регламентів, що визначають порядок управління ризиками в державних установах. Такі політики повинні чітко регламентувати процеси виявлення ризиків, порядок їх оцінки, відповідальність конкретних осіб та механізми контролю. Для прикладу, в багатьох країнах діють обов’язкові стандарти оцінки ризиків для всіх об’єктів критичної інфраструктури, що забезпечує уніфікований підхід до кіберзахисту на загальнодержавному рівні.

Особливе значення має проактивний моніторинг та прогнозування загроз. Використання систем аналізу поведінки користувачів (UBA), технологій машинного навчання та штучного інтелекту дозволяє не тільки виявляти підозрілі дії, а й передбачати потенційні сценарії атак. Це забезпечує випереджальне реагування, коли інцидент попереджається ще до його фактичної реалізації.

Запобіжні заходи не можуть бути ефективними без активної роботи з персоналом. Політики ризик-менеджменту повинні включати регулярні тренінги з кібергігієни, навчання розпізнаванню фішингових листів, перевірку обізнаності співробітників через контрольовані тестові атаки.

Варто підкреслити, що ризик-менеджмент у державному секторі має також стратегічний вимір. Він не зводиться лише до технічних чи організаційних аспектів, а включає формування довгострокових підходів до планування ресурсів, розробку сценаріїв дій у разі кризових ситуацій, а також координацію з іншими державами та міжнародними організаціями. Це особливо актуально в умовах зростання кількості кібератак, які мають геополітичний характер і можуть бути елементом гібридних війн.

Загалом, запобіжні заходи та політики ризик-менеджменту є невід’ємною частиною комплексної системи кіберзахисту державного сектору. Вони дозволяють створювати бар’єри для потенційних загроз, мінімізувати вразливості та забезпечувати сталий розвиток цифрової інфраструктури держави. Їх ефективна реалізація не лише знижує ймовірність виникнення інцидентів, а й формує основу для довготривалої стійкості державного управління в умовах динамічного й агресивного кіберсередовища.

РОЗДІЛ 3. АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДЕРЖАВНОМУ СЕКТОРІ УКРАЇНИ

3.1. Оцінка ефективності державної політики в сфері інформаційної безпеки

Починаючи практичну оцінку ефективності державної політики в сфері інформаційної безпеки, необхідно спиратись винятково на кількісні показники й оперативні результати реалізованих стратегій та програм; нижче наводжу детальний аналітично-статистичний опис поточного стану (факти — з офіційних звітів державних органів та верифікованих публікацій), короткі інтерпретації цих показників і таблицю з ключовими метриками для 2023–2024 років.

У 2024 році загальна статистика інцидентів у державному інформаційному просторі показала різке загострення: офіційні дані та оперативні підрахунки свідчать про 4 315 зареєстрованих кіберацидентів у 2024 році проти 2 541 у 2023-му, що відповідає зростанню близько 69,8% (рік до року). Такий стрибок є кількісним виразом інтенсифікації атак і одночасно віддзеркалює підвищену здатність систем виявляти та реєструвати події.

Одночасно державні оперативні служби фіксують інші, більш «аналітичні» показники: операційні центри реагування повідомляють, що в 2024 році в межах Системи виявлення вразливостей і реагування на кіберінциденти було опрацьовано майже 3 мільйони подій телеметрії, із яких аналітично виокремлено близько 28 тисяч критичних подій і безпосередньо опрацьовано 1 042 кіберінциденти спеціалістами Оперативного центру реагування. Важливо підкреслити, що різниця між «зареєстрованими подіями/інцидентами» у загальній звітності і «опрацьованими аналітичною командою інцидентами» пояснюється методологією (первинна телеметрія → фільтрація → критичні події → інциденти, що вимагають оперативного втручання).

Масштаби моніторингу та технічного покриття 2024 року, теж, підвищилися: кількість захищених хостів у системі моніторингу перевищує 28

тисяч робочих станцій і серверів, до підсистем NDR/EDR/ASM підключено десятки організацій (включно з новими підключеннями протягом року), що дозволило значно розширити «дзеркало» кіберпростору для аналітики та оперативного реагування. Ці технічні показники свідчать про реальні зусилля з масштабування можливостей виявлення, але не усувають викликів у сфері покриття всіх критичних об’єктів.

Структура атак і розподіл за мішенями мають практичне значення для оцінки прикладних результатів політики. В 2024 році основними цілями атак були місцеві органи влади, урядові установи, сектор безпеки й оборони, енергетика, комерційні організації та телекомунікації; найпоширеніші вектори — розповсюдження шкідливого програмного забезпечення, фішинг, шкідливі з’єднання (malicious connection) та компрометація облікових записів. Така конфігурація мішеней прямо впливає на пріоритезацію заходів: удар першочергово має припадати на підсилення захисту урядових та енергетичних систем і на механізми захисту облікових записів.

З точки зору державного планування, у грудні 2023 року було формально затверджено план заходів на 2023–2024 роки із реалізації Стратегії кібербезпеки, у якому закладено такі прикладні цілі: створення системи індикаторів стану кібербезпеки, формування кібервійськ в рамках Міноборони, встановлення механізмів взаємодії між суб’єктами національної системи кібербезпеки, розробка плану кібероборони й проведення навчань у співпраці з партнерами НАТО. План вимагає від відповідних органів регулярної звітності й передбачає конкретні строки виконання окремих заходів. Факт наявності цього плану дає формальні підстави для вимірювання прогресу, проте його практична реалізація потребує порівняльного зіставлення з фактичними показниками підключення об’єктів, темпами навчань та результатами аудиту.

Паралельно з державними програмами спостерігається інтенсивне зростання ринку кібербезпеки, що є індикатором мобілізації приватних ресурсів та появи нових постачальників послуг: за оцінками ринку, обсяг національного ринку кібербезпеки у 2024 році становив близько $138 млн, що означає помітне

розширення індустрії й потенціал для аутсорсингу частини функцій захисту для державних установ. Це має практичне значення при плануванні централізованих закупівель і партнерств.

Нижче наведена таблиця 3.1 з ключовими статистичними показниками, які дозволяють кількісно зіставити результати реалізації стратегій і програм у 2023–2024 роках.

Таблиця 3.1

Ключові статистичні показники реалізації стратегій і програм кіберзахисту в Україні

Показник (метрика)	**Значення 2023**	**Значення 2024**
Зареєстровані кібератаки / інциденти (загальний підрахунок)	2 541	4 315
Кількість інцидентів, опрацьованих аналітично (OCRC / CBB)	—	1 042
Кількість подій телеметрії, підданих аналізу	—	≈ 3 000 000
Кількість захищених хостів (EDR-покриття)	—	>28 000 хостів
Частка інцидентів, що стосуються урядового сектору	—	>90% серед опрацьованих інцидентів
Найпоширеніші вектори атак	—	Malware, Phishing, Malicious connection, Compromised accounts

Продовження таблиці 3.1

Наявність плану заходів (реалізація стратегії)	План затверджено (грудень 2023)	План в дії (терміни 2023–2024)
Оцінка ринкового ресурсу (приблизно)	—	$138 млн (оціночний ринок кібербезпеки, 2024)

Після зіставлення чисел очевидні кілька практично важливих висновків. По-перше, різке збільшення числа зафіксованих інцидентів у 2024 році (≈+70%) не лише відображає загострення загрози, а й частково свідчить про розширення можливостей моніторингу та реєстрації подій, оскільки значні обсяги телеметрії й додаткові підключення сенсорів дали змогу виявляти більше «раніше невидимих» подій; разом із тим абсолютне зростання інцидентів створило надмірне навантаження на аналітичні центри реагування.

По-друге, операційна спроможність центрів реагування (OCRC / CSIRT) у 2024 році була доповнена технічними можливостями (NDR/EDR/ASM), але кількість організацій, які підключені до цих підсистем, і масштаби охоплення залишаються обмеженими порівняно з кількістю об’єктів критичної інфраструктури по всій території країни; це створює «прогалини» в зоні раннього виявлення й потребує прискореного масштабування підключень.

По-третє, секторний розподіл інцидентів підтверджує, що урядові й енергетичні системи перебувають у зоні підвищеного ризику, отже ефективність програм слід вимірювати не лише загальними індикаторами (кількість інцидентів), а й інструментами захисту критичних секторів (часи реакції на інциденти у секторі, ступінь сегментації мереж, наявність автономних резервних сценаріїв).

Наявність національного плану заходів (КМУ №1163-р) дає чіткі контрольні точки (індикатори стану кібербезпеки, створення кібервійськ, міжвідомча взаємодія, навчання з партнерами НАТО), проте для практичної оцінки реалізації необхідно звіряти ці формальні маркери з фактичними показниками підключення об’єктів, частотою навчань та звітами про спільні

вправи. Іншими словами, формальна наявність плану вже створює основу для вимірювання, але реальна ефективність визначається виконанням конкретних технічних і кадрових метрик.

Короткий приклад прикладної інтерпретації: якщо в 2024 році система виявила й опрацювала 3 млн одиниць телеметрії і 1 042 інциденти, але понад 90% інцидентів стосувалися урядового сектору, то практичний висновок полягає у необхідності пріоритезації ресурсів на уніфіковані засоби захисту саме урядових реєстрів і сервісів (каскадне резервування, жорстка MFA, сегментація та EDR для робочих станцій із високим рівнем доступу). Такий висновок можна верифікувати шляхом порівняння частоти інцидентів до/після підключення конкретних підсистем у кожній організації.

В Європейському Союзі ключовим інструментом формалізації очікувань від держав і операторів є Директива NIS2 та суміжні продукти ENISA, які розширили коло об'єктів, що підлягають обов'язковим вимогам безпеки, уточнили правила інформування про інциденти та ввели уніфіковані технічні й організаційні стандарти для критичних і важливих секторів. Практика імплементації NIS2 показує, що жорсткіші вимоги до звітності і до адміністрування ризиків змушують держави посилювати міжвідомчу координацію і вводити чітко вимірювані KPI для підзвітних організацій, зокрема строки повідомлення про інциденти та мінімальні вимоги до управління ризиками. Цей підхід дає змогу не лише підвищити прозорість загроз, але й покращити швидкість реакції при масштабних атаках, оскільки створює формальні канали обміну інформацією та юридичну відповідальність за невиконання вимог.

Модель Сполучених Штатів базується на поєднанні стандартів ризик-менеджменту (NIST Cybersecurity Framework і RMF) та сильної ролі операційного центру на федеральному рівні (CISA), який одночасно надає технічну допомогу, координує розслідування і видає практичні посібники для штатів і органів місцевого уряду. Практичний висновок з американського досвіду — поєднання універсальної рамки управління ризиками (яка дає спільну

мову для державних і приватних структур) із реальною інституцією, котра має повноваження і ресурси надавати оперативну допомогу під час інцидентів, суттєво підвищує оперативну спроможність відповіді та скорочує час від виявлення до відновлення. В США, теж, широко використовують підходи «playbook-oriented» реагування і формалізоване залучення федеративних ресурсів для відновлення критичних сервісів.

У Великій Британії практичні програми NCSC показують, як державні сервіси можуть надати підприємствам і державним органам конкретні, готові до вживання інструменти — від безкоштовних сервісів Active Cyber Defence (сканування зовнішніх векторів, автоматичні блокування фішингових доменів і т. п.) до настанов з простої кібергігієни (програма Cyber Essentials). Досвід Великої Британії підкреслює, що державні інструменти «нижчого порогу входу» (low-barrier services), які легко впроваджуються малими та середніми структурами, підвищують загальний рівень стійкості екосистеми і водночас економлять ресурси на масове навчання й підтримку. Така операційна орієнтація дозволяє швидко знизити ризики, що залежать від базової конфігурації та налаштувань, не очікуючи повної модернізації інфраструктури.

Естонський досвід є прикладом комплексної практичної трансформації після масованих атак 2007 року: держава інвестувала у «security by design» при цифровізації послуг, розвила національні CERT/CSIRT, створила систему резервування критичних сервісів і запровадила модель, де волонтерські та резервні кіберпідрозділи (надбудовані над цивільними та оборонними структурами) доповнюють державні сили. Практичний ефект естонської моделі проявляється у високій готовності до масштабних атак, у швидкій відбудові сервісів та у стабільному нарощуванні локального кадрового пулу через участь громадян і приватного сектору у навчаннях і операціях. Для держав із обмеженими ресурсами така модель показує, що поєднання централізованого планування та децентралізованого залучення експертів дає помітний коефіцієнт віддачі.

Міжнародна співпраця і регулярні багатонаціональні вправи — ще один практичний компонент, який демонструє ефективність на полі операційної готовності. Прикладом є щорічні «live-fire» вправи Locked Shields від NATO/CCDCOE, які у реалістичних умовах моделюють масовані атаки на державні та критичні системи і дозволяють відточувати не лише технічні навички, а й координацію, юридичні процедури й комунікацію в кризі. Учасництво у таких вправах підвищує здатність швидко орієнтуватися в складних сценаріях і виробляє стандарти взаємодії, які потім транслюються в національні playbook-и. Цей практичний інструмент доводить, що вправи на живій інфраструктурі суттєво скорочують час навчання команд реагування і виявляють організаційні «вузькі місця», недоступні для виявлення при настільних тренуваннях.

Окремими державами (зокрема Сінгапуром та Ізраїлем) вироблено практичні моделі поєднання державних стратегій із індустріальними ініціативами: Сінгапур через Cyber Security Agency (CSA) реалізує цілу низку ініціатив для захисту державних і приватних OT/IT систем, включно з майстер-планом з кібербезпеки для промислових об’єктів та компетентнісними рамками для працівників. Ізраїль, навпаки, показує сильну модель формування кадрового резерву через військові підрозділи (наприклад, Unit 8200) і подальшу комерціалізацію експертизи в приватний сектор; практичним ефектом є швидкий розвиток локального ринку кібербезпеки та постійний притік висококваліфікованих фахівців у державні і приватні проекти. Для державного сектору такі приклади важливі тим, що демонструють життєздатні шляхи побудови кадрового потенціалу та створення елементів національної екосистеми кібербезпеки.

Синтез практичних уроків у пріоритетному вигляді дає такі висновки, які випливають безпосередньо з описаних прикладів: по-перше, централизація стратегічного управління при одночасній делегованій операційній реалізації (національна координація + відомчі CSIRT/SOC + приватні провайдери) підвищує ефективність реагування; по-друге, обов’язкові норми звітності та зрілі

механізми обміну розвідданими про загрози (технічний feed і юридичні механізми) покращують видимість і зменшують час виявлення; державні «низькопорогові» сервіси (як у Британії) і централізовані інструменти (EDR/NG-firewalls, threat intelligence платформі) швидко підвищують базовий рівень захищеності без довгих проєктів модернізації; регулярні масштабні live-fire вправи і симуляції (як Locked Shields) критично важливі для відпрацювання координації і процесів; розвиток кадрового потенціалу слід будувати одночасно через освіту, залучення військових/волонтерських ініціатив та заохочення приватного ринку до партнерств із державою.

Що з цієї практики прямо застосовне до України і які оперативні пропозиції випливають із міжнародного досвіду? Перше, введення обов'язкових правил швидкого повідомлення про інциденти і чітких SLA для первинної реакції (індикатори відповідності на кшталт NIS2) дозволить зменшити «вакуум» інформації між організаціями й національними центрами. Друге, масштабування підключень до централізованих NDR/EDR/telemetry платформ і розвиток регіональних SOC у поєднанні з централізованим CERT/CSIRT підвищить видимість без значних додаткових витрат на повну модернізацію інфраструктури кожної установи. Далі, державні «пакети» низького порога (автоматичні сканування зовнішніх атак, безкоштовні інструменти фільтрації фішингу, шаблони політик для MFA і патч-менеджменту) значно підвищать базову гігієну у державному секторі. Регулярні масштабні вправи за форматами Locked Shields та table-top сценарії з міжнародним залученням дозволять виявити організаційні «слабкі місця» до настання реального інциденту. Ну і, системний розвиток кадрового резерву — через програми освіти, стажування в CERT/CSIRT, волонтерські ініціативи та співпрацю з оборонними підрозділами — дасть стійкий кадровий фундамент, який підкріпить усі технічні заходи. Підставами для цих практичних порад є згадані міжнародні стандарти, операційні центри та вправи.

3.2. Практичні аспекти інформаційної безпеки в державних органах України

Рівень фактичного захисту інформаційних систем державних органів України значною мірою відображає як прогалини, так і досягнення у впровадженні практичних заходів кіберзахисту. Після активної цифровізації державних послуг (зокрема запуску платформи «Дія» та електронного документообігу в багатьох установах), питання реальної стійкості до атак стало одним із найважливіших. Масовані кібератаки на урядові ресурси у 2017 році («NotPetya») та у 2022 році на тлі військової агресії рф продемонстрували, що державні інформаційні системи залишаються ключовою ціллю та часто вразливими через недостатню інтеграцію сучасних інструментів безпеки, а також обмежені кадрові ресурси.

Аналітичні дані CERT-UA, Держспецзв'язку та звітів міжнародних партнерів дозволяють окреслити кілька характеристик рівня захищеності:

- Системи державного сектору в основному захищені базовими інструментами (антивірусні рішення, міжмережеві екрани), проте лише близько третини органів влади мають розгорнуті комплексні SIEM/SOC-рішення.
- Регулярні аудити та пентести проводяться точково, здебільшого в центральних органах, тоді як на місцевому рівні практика системної перевірки відсутня.
- Сегментація мереж і резервне копіювання впроваджені нерівномірно: частина установ має налаштовані системи резервування, проте у багатьох випадках ці копії зберігаються в незахищених середовищах.
- Рівень захисту персональних даних часто не відповідає сучасним вимогам: значна частина баз працює на застарілому програмному забезпеченні без регулярних оновлень.

— Навчання персоналу здійснюється епізодично, що знижує ефективність навіть тих інструментів, які вже розгорнуті.

Щоб краще відобразити ситуацію, подано таблицю 3.2.

Таблиця 3.2

Оцінка рівня захисту інформаційних систем державних органів України

Критерій захисту	**Рівень впровадження (у % державних органів)**	**Коментарі та проблемні аспекти**
Використання базових засобів (антивірус, фаєрвол)	~85%	Поширені майже у всіх центральних органах, однак часто відсутня централізована координація.
Впровадження SIEM/SOC-рішень	~30%	Притаманне переважно центральним органам влади; більшість місцевих структур не мають сучасних систем моніторингу.
Регулярні аудити та пентести	~25%	Виконуються точково, здебільшого у великих держустановах; відсутня уніфікована практика.
Сегментація мереж і резервне копіювання	~40%	Частково реалізовано; резервні копії часто зберігаються у тій самій мережі, що й основні системи.

Продовження таблиці 3.2

Захист персональних даних	~35%	Використовуються застарілі програмні комплекси, що ускладнює захист.
Системне навчання персоналу з ІБ	~20%	Тренінги проводяться нерегулярно, здебільшого разово або у формі семінарів без практичних кейсів.

Аналіз показує, що основні слабкі місця полягають у недостатній автоматизації процесів кіберзахисту, низькому рівні інтеграції передових технологій і відсутності системного підходу до підвищення кваліфікації персоналу. Водночас позитивним аспектом є те, що у центральних органах влади активно впроваджуються SOC-рішення, створюються механізми взаємодії з CERT-UA та запускаються спільні проєкти з міжнародними партнерами, які поступово підвищують рівень загальної кіберстійкості.

Далі, варто розглянути приклади реальних подій, які дозволяють оцінити, наскільки на практиці працюють впроваджені інструменти, які помилки допускаються у кризових обставинах і які рішення виявляються найефективнішими.

Серед найбільш успішних прикладів варто відзначити створення Національного центру резервування даних, який дозволив забезпечити безперервність роботи критичних реєстрів навіть під час масштабних кібератак у 2022 році через війну. Попри спроби деструктивного втручання у державні сервіси, більшість ключових баз даних — зокрема реєстри Міністерства юстиції та платформи на кшталт «Дія» — залишилися доступними для громадян. Це стало можливим завдяки впровадженню віддалених дата-центрів, багаторівневому резервуванню та координації між Держспецзв’язку й міжнародними партнерами. Успішним, також, можна вважати кейс синхронізації роботи CERT-UA з урядовими установами, коли завдяки оперативним

повідомленням про фішингові кампанії вдалося знизити рівень їх ефективності: у низці відомств показник «клікрейт» співробітників скоротився майже вдвічі протягом пів року.

Водночас, у практиці траплялися й невдалі випадки, що підсвітили вразливість систем. Найбільш резонансним лишається, вищезгаданий, інцидент із поширенням вірусу-шифрувальника «NotPetya» у 2017 році. Він паралізував роботу багатьох державних установ, зокрема фінансових і транспортних структур, а збитки оцінювалися в сотні мільйонів доларів. Основними причинами стали відсутність належного патч-менеджменту та слабка сегментація мереж, що дозволило шкідливому коду швидко поширитися. Схожі проблеми виявилися й у 2022 році, коли низка державних сайтів зазнала атак типу «deface» із масовим виведенням деструктивних повідомлень. Хоча ці атаки не призвели до суттєвих втрат даних, вони мали потужний психологічний ефект та показали недостатність механізмів оперативного відновлення репутаційної стабільності ресурсів.

3.3. Проблеми та недоліки сучасної системи інформаційної безпеки

Однією з ключових проблем є відсутність єдиного системного кодексу або узагальненого закону, який би комплексно регулював сферу кібер- та інформаційної безпеки. Сьогодні норми розпорошені між законами «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних» та низкою підзаконних актів. Це створює правову невизначеність, коли одні й ті самі питання (наприклад, процедури обробки даних або вимоги до захисту інформаційних систем) регламентуються різними документами, що нерідко призводить до колізій.

Важливою проблемою є й повільна імплементація міжнародних стандартів, насамперед ISO/IEC 27001, NIST Cybersecurity Framework та GDPR-практик. Хоча у стратегічних документах їхнє врахування декларується,

фактична інтеграція залишається обмеженою. Це негативно позначається на взаємодії з міжнародними партнерами, а також ускладнює захист персональних даних громадян при транскордонному обміні інформацією.

Крім того, нормативна база страждає від недостатньої деталізації процедур реагування на кіберінциденти. Закон «Про основні засади забезпечення кібербезпеки України» лише загально визначає компетенції відповідальних органів, проте не встановлює чітких SLA (Service Level Agreements) щодо часу виявлення, ескалації та ліквідації інцидентів. Це призводить до ситуацій, коли різні установи реагують за власними внутрішніми процедурами, і ефективність взаємодії значно знижується.

Ще одним проблемним аспектом є фінансування заходів кіберзахисту. Хоча у законах декларується необхідність виділення коштів, відсутні нормативно закріплені механізми обов'язкового бюджетного планування кібербезпеки. В результаті витрати на ІБ у різних органах коливаються від 0,5% до 3% загального ІТ-бюджету, тоді як у країнах ЄС цей показник сягає 10–15%.

Для більшої наочності ключові проблеми узагальнено в таблиці 3.3.

Таблиця 3.3

Основні проблеми нормативного регулювання у сфері інформаційної безпеки України

Категорія проблеми	**Суть недоліку**	**Аналітичні наслідки**
Фрагментарність законодавства	Відсутність єдиного комплексного акту; дублювання норм у різних законах	Правова невизначеність, колізії у трактуванні
Низька імплементація міжнародних стандартів	Обмежене застосування ISO/IEC 27001, NIST, GDPR	Ускладнена інтеграція з міжнародними партнерами; ризики транскордонного обміну

Таблиця 3.3

Недостатня деталізація реагування на інциденти	Відсутність чітких SLA та єдиних процедур	Зниження ефективності координації між органами
Проблеми фінансування	Відсутність закріпленого механізму планування бюджету на ІБ	Низька частка витрат на кіберзахист (0,5–3% ІТ-бюджету проти 10–15% у ЄС)
Повільність оновлення законодавства	Тривалі процедури ухвалення змін	Відставання від динаміки появи нових кіберзагроз

В цілому, аналіз показує, що нормативно-правова база у сфері інформаційної безпеки України поки що не виконує повною мірою роль фундаменту для ефективного функціонування системи кіберзахисту. Її недоліки спричиняють розрив між стратегіями та їхньою практичною реалізацією, що створює додаткові ризики для державних органів і громадян. Також, аналіз інцидентів останніх років показує, що найбільшою слабкістю української системи кіберзахисту є не відсутність технологій чи коштів, а саме недосконала взаємодія між установами. В окремих випадках ця проблема мала відчутні наслідки.

За даними CERT-UA, у 2022 році понад 40% виявлених кібератак на державні інформаційні ресурси не були вчасно ескаловані від регіональних підрозділів до центральних органів. У середньому, час передачі повідомлення про інцидент із місцевого рівня до центрального складав 36–48 годин, тоді як міжнародна практика вимагає від кількох хвилин до 2 годин. Це створювало вікно уразливості, яким активно користувалися зловмисники.

Ще один приклад — масові DDoS-атаки на урядові сайти у лютому-березні та протягом літа 2022 року. Хоча центральні органи змогли відновити роботу

більшості ресурсів за 6–8 годин, регіональні портали держпослуг залишалися недоступними в середньому від 24 до 48 годин. Це пояснювалося тим, що місцеві ІТ-підрозділи не мали прямого каналу для отримання рекомендацій від Національного координаційного центру кібербезпеки, і змушені були діяти самостійно.

Проблеми координації виявилися і в питаннях звітності про кіберінциденти. Наприклад, у 2023 році різні міністерства подали понад 120 звітів про атаки фішингового характеру, проте близько 30% із них містили неповні або дубльовані дані. Відсутність уніфікованої системи обліку призводить до того, що ресурси витрачаються на обробку дублюючої інформації, замість того щоб концентруватися на реальних загрозах.

Також, варто відзначити питання міжнародної співпраці. За інформацією з відкритих звітів ENISA (Європейського агентства з кібербезпеки), лише близько 15% українських держустанов мають налаштовані прямі інтеграційні канали обміну кіберрозвідданими з європейськими партнерами. Це означає, що в більшості випадків обмін відбувається через кілька проміжних інстанцій, що знижує швидкість отримання критичних попереджень.

Але окрім цього всього, ще серйознішою перешкодою для побудови надійної системи інформаційної безпеки є обмежене фінансування та застаріла матеріально-технічна база багатьох органів влади.

За офіційними даними Державної служби спеціального зв’язку та захисту інформації, у 2022–2024 роках на програми кіберзахисту в державному секторі виділялося в середньому близько 0,08% від державного бюджету, тоді як у країнах ЄС ця частка коливається від 0,25% до 0,4%. Така диспропорція створює відставання у фінансуванні в кілька разів, що напряму позначається на спроможності державних органів протистояти сучасним загрозам.

Для прикладу, аудит, проведений у 2024 році в центральних органах виконавчої влади, показав, що понад 60% серверного обладнання використовується більше 7 років, тоді як рекомендований термін експлуатації для систем, що обробляють критично важливу інформацію, складає 3–5 років.

Це означає, що багато систем уже не підтримуються виробниками, не отримують оновлень безпеки та стають потенційною мішенню для кібератак.

Крім того, понад 40% державних установ у регіонах України працюють на ліцензійному програмному забезпеченні, яке давно втратило офіційну підтримку, а близько 20% — на неліцензійному або безкоштовному ПЗ, яке не відповідає стандартам кіберзахисту. Це призводить до того, що при виникненні загроз технічні спеціалісти не мають змоги швидко застосувати оновлення чи отримати технічну підтримку від виробників.

Важливим чинником є й кадровий аспект, тісно пов’язаний із фінансуванням. За даними дослідження Українського інституту кіберполітики (2023 р.), середня зарплата спеціаліста з інформаційної безпеки в державному секторі становила від 18 до 25 тис. грн, тоді як у приватному секторі вона перевищувала 60–70 тис. грн. Це створює суттєвий відтік кваліфікованих кадрів у комерційні структури, залишаючи державні органи з дефіцитом висококласних фахівців, незважаючи на наявність обладнання чи формальних програм.

Таблиця 3.4

Основні проблеми фінансування та технічного забезпечення в держсекторі

Показник	Дані	Наслідки
Частка бюджету на кіберзахист	~0,08% від держбюджету	У 3–4 рази менше, ніж у країнах ЄС
Стан серверного обладнання	60% працює понад 7 років	Відсутність оновлень безпеки, високий рівень уразливості
Використання ліцензійного, але застарілого ПЗ	40% установ	Неповна сумісність із сучасними стандартами

Продовження таблиці 3.4

Використання неліцензійного/безкоштовного ПЗ	~20% установ	Відсутність підтримки виробників, високий ризик атак
Рівень зарплат у сфері ІБ	18–25 тис. грн у держсекторі проти 60–70 тис. грн у приватному	Відтік кадрів, дефіцит спеціалістів

Загалом, статистика чітко показує, що проблема фінансування та технічного забезпечення є системною й багатовимірною: вона стосується не лише недостатнього обсягу коштів, але й їх неефективного використання, застарілої інфраструктури та нерівних умов оплати праці для фахівців. А сукупність цих всіх факторів робить державний сектор вразливішим у порівнянні як з міжнародними партнерами, так і з власним приватним сектором, де рівень кіберзахисту суттєво вищий.

РОЗДІЛ 4. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДЕРЖАВНОМУ СЕКТОРІ

4.1. Пропозиції щодо вдосконалення законодавчої бази

Аналіз практики останніх років свідчить, що навіть за умови поступового розвитку національної системи інформаційної безпеки Україна стикається з фундаментальною проблемою — відсутністю єдиної, цілісної й сучасної законодавчої бази, яка б відповідала викликам цифрової доби. Наявні норми розпорошені по різних актах, часто дублюють одна одну, суперечать між собою або не враховують швидких змін у технологічному середовищі. У результаті навіть достатні зусилля державних органів чи окремих підрозділів втрачають ефективність, оскільки вони діють у правовому полі, яке більше стримує, ніж сприяє розвитку. Саме тому розробка нових правових норм стає ключовим напрямом удосконалення державної політики в сфері інформаційної безпеки.

В першу чергу мова йде про необхідність кодифікації законодавства, тобто ухвалення єдиного комплексного закону «Про інформаційну безпеку та кіберзахист». Такий документ мав би стати основою для всієї системи, уніфікувати термінологію, чітко визначити коло суб’єктів, їхні повноваження та відповідальність, а також закріпити принципи ризик-орієнтованого управління в інформаційній сфері. Кодифікований акт дозволив би усунути суперечності, зменшити правову невизначеність та створити прозорі правила гри як для державних органів, так і для суб’єктів критичної інфраструктури.

Окремої уваги потребує питання правового регулювання процесу реагування на кіберінциденти. Досвід показує, що затримки з передачею інформації та дублювання звітів у різних структурах суттєво знижують здатність держави протистояти загрозам. Тому нові норми повинні передбачати чіткі строки повідомлення про інциденти, обов’язкові для всіх суб’єктів, а також визначити єдину форму і канал комунікації. Юридичне закріплення таких правил

створить умови для миттєвої ескалації інформації та дозволить скоротити час реакції з діб до кількох годин чи навіть хвилин.

Не менш важливою є проблема обліку та класифікації об’єктів критичної інформаційної інфраструктури. На сьогодні в Україні відсутній уніфікований реєстр, що ускладнює розподіл ресурсів та не дозволяє будувати адекватні стратегії захисту. Нове законодавство повинно запровадити обов’язкову реєстрацію об’єктів КІІ, встановити чіткі критерії віднесення систем до тієї чи іншої категорії критичності та визначити відповідні мінімальні вимоги до їхнього захисту. Це дозволить державі зосереджувати зусилля насамперед на найбільш чутливих і вразливих сегментах, а також забезпечить прозорість у питаннях пріоритезації фінансування.

Законодавче врегулювання потребує також технічний бік питання. Йдеться про визначення обов’язкових базових заходів кібергігієни для всіх державних установ: багатофакторної автентифікації для доступу до критичних систем, регулярного оновлення програмного забезпечення, створення резервних копій за міжнародними стандартами, обов’язкової сегментації мереж і проведення незалежних аудитів безпеки. Така норма має бути універсальною, тобто поширюватися навіть на найменші органи місцевого самоврядування, що працюють з персональними даними або мають доступ до державних інформаційних ресурсів.

Водночас розробка нових правових норм не може обійтися без фінансового блоку. Обмежене фінансування, що сьогодні становить лише соті частки відсотка державного бюджету, не здатне забезпечити навіть мінімальні потреби системи. Саме тому у законодавстві слід закріпити норму про обов’язкове виділення визначеної частки бюджету на інформаційну безпеку в кожному органі державної влади. Доречним виглядає також створення Фонду кіберстійкості, кошти якого могли б використовуватися для швидкого реагування на інциденти, централізованих закупівель сучасного обладнання чи фінансування термінових заходів після масштабних атак.

Важливим нововведенням у правовій площині має стати інтеграція принципу «secure-by-design» у сферу державних закупівель. Це означає, що при виборі програмного забезпечення або обладнання ключовим критерієм має бути не лише ціна, а й відповідність міжнародним стандартам безпеки, проходження незалежної сертифікації та перевірка постачальника. Подібна норма дозволить мінімізувати ризики, пов’язані з ланцюгами постачання, що особливо актуально у світлі сучасних атак на глобальні технологічні компанії.

Не можна оминути і питання захисту персональних даних, адже сучасні державні електронні сервіси щодня обробляють мільйони записів громадян. Нові правові норми мають бути гармонізовані з європейським законодавством у сфері захисту даних, зокрема з вимогами GDPR. Це не лише підвищить рівень довіри громадян до електронних послуг, а й відкриє Україні можливості для тіснішої інтеграції у цифровий простір ЄС.

Окремо, варто підкреслити важливість закріплення у законодавстві обов’язкової прозорої звітності щодо стану кіберзахисту. Кожен орган державної влади повинен щорічно публікувати стандартизований звіт, який міститиме інформацію про кількість зафіксованих інцидентів, швидкість їхнього реагування, рівень впровадження базових засобів захисту та результати незалежних аудитів. Така звітність, по-перше, забезпечить громадський контроль, а по-друге, дозволить уряду й парламенту об’єктивно оцінювати динаміку та приймати обґрунтовані рішення щодо подальших кроків.

З огляду на швидкість розвитку технологій нові правові норми мають включати положення про адаптивність, тобто передбачати регулярний перегляд і оновлення. Це дозволить уникнути ситуації, коли закон уже через два-три роки після ухвалення стає застарілим. Найбільш ефективним є закріплення обов’язку уповноваженого органу щорічно готувати пропозиції щодо актуалізації нормативної бази з урахуванням нових викликів і загроз.

Далі, не менш важливим завданням постає узгодженість правових норм із міжнародними нормами та стандартами. Бо в умовах глобалізованого цифрового простору національна ізольованість у сфері правового регулювання кіберзахисту

неминуче призводить до вразливостей. Україна, що активно рухається в напрямку євроінтеграції, має забезпечити відповідність власних законодавчих положень вимогам і практикам, які вже усталилися в міжнародній спільноті. Лише тоді держава зможе ефективно брати участь у колективних системах протидії кіберзагрозам і отримувати повноцінний доступ до партнерських механізмів реагування.

Насамперед, питання гармонізації стосується зближення українських правових норм із регламентами Європейського Союзу. Особливе значення має імплементація положень Директиви NIS2 (Network and Information Security Directive), яка зобов'язує держави-члени створювати національні стратегії кібербезпеки, визначати критичні об'єкти інфраструктури, формувати вимоги до звітності про інциденти й забезпечувати координацію між усіма суб'єктами системи. Впровадження аналогічних положень в українське законодавство дозволить побудувати узгоджену систему кіберзахисту, яка органічно інтегрується в європейський простір.

Важливим аспектом є й захист персональних даних. Європейський регламент GDPR сьогодні став світовим еталоном у сфері прав громадян на конфіденційність і контроль над власними даними. В Україні вже існують окремі законодавчі акти, які частково регулюють це питання, однак їхня ефективність обмежена через відсутність реальних механізмів примусу та дієвих санкцій. Тому гармонізація передбачає не лише адаптацію термінології чи окремих процедур, а й запровадження дієвої інституційної моделі контролю, включаючи незалежний орган із нагляду за дотриманням правил обробки персональних даних. Це підвищить довіру громадян до електронних державних послуг і водночас відкриє Україні шлях до тіснішої співпраці в цифровій сфері з країнами ЄС.

Варто, теж, відзначити значення міжнародних стандартів, таких як ISO/IEC 27001, які встановлюють комплекс вимог до управління інформаційною безпекою. У країнах Європейського Союзу і НАТО ці стандарти є базовим орієнтиром при організації систем захисту, і саме їхнє поступове впровадження

в українську практику дає змогу формувати універсальну мову взаємодії з партнерами. Закріплення в національному законодавстві вимоги щодо відповідності державних органів і суб'єктів критичної інфраструктури міжнародним стандартам управління безпекою сприятиме підвищенню сумісності систем і полегшить інтеграцію у спільні кіберзахисні ініціативи.

Крім того, гармонізація потребує і політичного, і процедурного наповнення. Необхідно створити механізм регулярного оновлення українських правових норм відповідно до змін у міжнародних документах. Це може бути реалізовано у формі спеціалізованої експертної ради при профільному міністерстві, яка б щороку готувала звіти щодо змін у світових стандартах та пропонувала відповідні оновлення у національній правовій базі. Такий підхід забезпечить динамічність і дозволить уникати правової стагнації.

Особливу увагу потрібно звернути на координаці. з міжнародними організаціями, які вже давно працюють у сфері кіберзахисту. Йдеться про НАТО, яке має власний Центр передового досвіду з кібероборони в Таллінні, про Європейське агентство з кібербезпеки (ENISA), а також про численні міждержавні ініціативи. Для того, щоб Україна могла повною мірою користуватися цими можливостями, її правові механізми мають бути максимально близькими до тих, що вже діють у партнерів. Це стосується не лише технічних вимог, а й процедурних деталей, таких як стандартизовані форми повідомлень про кіберінциденти чи протоколи обміну інформацією.

Також, гармонізація українського законодавства з міжнародними стандартами має ще один важливий вимір — економічний. Бізнес, який працює на глобальних ринках, потребує передбачуваного та зрозумілого правового середовища. Якщо норми в Україні відповідатимуть європейським і світовим практикам, це стане додатковим фактором привабливості для іноземних інвесторів, які зможуть бути впевненими у захищеності даних і прозорості регуляторних процедур.

4.2. Використання інноваційних технологій для посилення захисту інформації

Сучасні виклики в сфері інформаційної безпеки дедалі частіше вимагають пошуку не лише організаційних чи правових рішень, а й інноваційних технологій, здатних кардинально підвищити рівень захищеності державних інформаційних систем. Однією з таких технологій є блокчейн, яка завдяки своїй децентралізованій структурі, прозорості й високому рівню захисту від несанкціонованих змін даних уже довела ефективність у фінансовій сфері та поступово інтегрується у практику державного управління різних країн. Для України, яка перебуває під постійним тиском кіберзагроз, застосування блокчейн-рішень може стати стратегічним інструментом підвищення стійкості та довіри до державних цифрових сервісів.

Перевага блокчейну полягає в тому, що інформація в системі зберігається у вигляді послідовного ланцюга блоків, кожен з яких захищений криптографічними методами й пов’язаний із попереднім. Це практично унеможливлює несанкціоноване редагування чи видалення даних, оскільки будь-яка зміна потребуватиме перезапису всього ланцюга одночасно на більшості вузлів мережі. Такий принцип дозволяє знизити ризик підробки документів, маніпуляцій з результатами електронних тендерів чи корупційних схем у сфері публічних фінансів.

Аналітичні дослідження підтверджують, що держави, які почали впроваджувати блокчейн у сфері публічного адміністрування, отримали відчутні результати. Для прикладу, Естонія використовує елементи цієї технології в системі захисту електронних реєстрів, що забезпечує повний контроль за доступом до персональних даних громадян і підвищує рівень довіри суспільства до електронних послуг. У Грузії блокчейн застосовується в земельному кадастрі, що дозволяє уникати шахрайства з правом власності та робить усі операції максимально прозорими.

З економічної точки зору блокчейн у державному секторі може суттєво скоротити витрати. За оцінками Світового банку, впровадження блокчейн-технологій у процеси документообігу здатне зменшити адміністративні витрати на 20–30 %, оскільки зникає потреба у великій кількості посередників і перевіряльних процедур. Для України це може означати не лише оптимізацію видатків бюджету, а й зниження рівня корупційних ризиків у сферах, де відбувається найбільший обіг інформації — наприклад, у податковій сфері, митниці чи державних закупівлях.

Не менш важливим є підвищення прозорості та довіри громадян до державних електронних сервісів. Використання блокчейн-технологій у реєстрах актів цивільного стану, системі е-голосування чи при адмініструванні соціальних виплат створює механізм, за якого жодна посадова особа не може непомітно змінити дані у власних інтересах. Це особливо актуально в умовах суспільної недовіри до державних інституцій: технологія може стати тим інструментом, який поступово відновлює довіру громадян завдяки абсолютній прозорості операцій.

Таблиця 4.1

Основні переваги впровадження блокчейн-технологій у державні інформаційні системи

Напрям застосування	**Потенційні вигоди для держави**	**Приклади з міжнародного досвіду**
Державні реєстри (кадастри, майнові)	Захист від шахрайства, неможливість підробки	Грузія – реєстр нерухомості на блокчейні
Електронні вибори	Гарантія прозорості результатів, мінімізація фальсифікацій	Естонія – е-голосування з блокчейн-захистом

Продовження таблиці 4.1

Податкові й митні операції	Автоматизація процесів, скорочення витрат і корупційних ризиків	США – пілотні проєкти в податковій сфері
Соціальні виплати та пільги	Контроль за цільовим використанням коштів, виключення дублювань	ОАЕ – програми адресної допомоги
Документообіг у держорганах	Зменшення адміністративних витрат на перевірку та зберігання	Великобританія – пілотні системи smart-contracts

Впровадження блокчейн-технологій у державні інформаційні системи є не лише технологічною інновацією, а й інструментом підвищення прозорості, стійкості та ефективності державного управління. Воно забезпечує мінімізацію ризиків кіберзагроз, оптимізацію витрат, зниження корупційних факторів і формування довіри громадян до цифрових сервісів.

Якщо блокчейн здатен гарантувати незмінність і прозорість даних у державних системах, то наступним ключовим кроком стає їхнє активне використання для прогнозування та нейтралізації загроз. В сучасних умовах кібератаки розвиваються настільки швидко, що традиційні методи захисту часто виявляються запізнілими. Тому технології Big Data та штучного інтелекту поступово стають основним інструментом для держав, які прагнуть перейти від реактивної до проактивної моделі кіберзахисту.

Використання великих масивів даних дозволяє виявляти аномалії у роботі інформаційних систем державних органів у реальному часі. Для прикладу, аналіз мільйонів логів з серверів та мережевого трафіку може показати підозрілі патерни поведінки, що вказують на початок кібератаки. За даними компанії *Accenture*, застосування аналітики Big Data знижує середній час виявлення інциденту з 206 днів (характерних для традиційних систем моніторингу) до 20–25 днів, а в поєднанні з алгоритмами машинного навчання цей показник може

бути скорочений до кількох годин. Для державних органів, які оперують критично важливою інформацією, подібна швидкість є питанням національної безпеки.

Штучний інтелект на основі аналізу великих даних дозволяє не лише фіксувати інциденти, а й прогнозувати ймовірність атак. Наприклад, алгоритми машинного навчання можуть будувати моделі поведінки користувачів у державних системах і виявляти відхилення, які потенційно вказують на внутрішні загрози. За статистикою *IBM Security*, понад 30 % витоків даних у державному секторі пов’язані саме з внутрішніми інсайдерами або недбалим ставленням працівників до правил безпеки. Використання AI-рішень дозволяє мінімізувати ці ризики завдяки безперервному моніторингу та автоматизованій оцінці рівня довіри до кожної дії користувача.

Особливу цінність Big Data та AI мають у сфері національних систем реагування на кіберінциденти. У США, наприклад, Національний центр з кіберзахисту щодня обробляє понад 30 мільярдів кіберподій, і без автоматизованого аналізу ці обсяги просто неможливо було б ефективно опрацьовувати. В Україні масштаби менші, проте навіть CERT-UA (урядова команда реагування на комп’ютерні надзвичайні події) щороку фіксує понад 200 тисяч спроб атак на державні інформаційні ресурси. Використання Big Data-аналітики могло б дозволити не лише швидше їх обробляти, а й формувати прогностичні моделі щодо напрямів майбутніх атак.

Позитивний ефект застосування технологій Big Data та AI можна продемонструвати на прикладі фінансового сектору, який часто виступає індикатором ефективності таких рішень. Ще у 2022 році Європейський центральний банк повідомив, що впровадження системи прогнозного аналізу на основі штучного інтелекту зменшило кількість успішних шахрайських транзакцій на 25 %. Якщо перенести цей досвід у державний сектор України, аналогічні рішення могли б суттєво знизити частоту фішингових атак, які становлять до 60 % усіх зареєстрованих інцидентів у вітчизняних держорганах.

Ще один важливий напрям застосування — створення системи кіберіндикаторів ризику, яка на основі Big Data буде формувати динамічні карти кіберзагроз у державному секторі. Це дозволить керівним органам не лише реагувати на інциденти, а й прогнозувати, які саме державні інституції опиняться під ударом найближчим часом. Подібна практика вже використовується у Великобританії в межах *National Cyber Security Centre*, де штучний інтелект у реальному часі моделює сценарії розвитку атак і попереджає установи ще до того, як відбудеться масштабне проникнення.

Для наочності ефективність використання Big Data та AI у сфері державної інформаційної безпеки зроблено таблицю 4.2.

Таблиця 4.2

Порівняння традиційних та інноваційних підходів до виявлення кіберзагроз у державному секторі

Параметр аналізу	**Традиційні методи моніторингу**	**Big Data + AI-рішення**
Середній час виявлення інциденту	150–200 днів	1–48 годин
Обсяг даних, що опрацьовуються	Обмежені (логи систем)	Мільярди записів на добу
Рівень точності у виявленні загроз	60–70 %	90–95 %
Виявлення внутрішніх загроз	Обмежені можливості	Прогностичні моделі поведінки
Потенціал прогнозування атак	Відсутній	Високий (аналітика трендів)

Продовженням цієї тенденції є автоматизація процесів контролю та моніторингу. Бо, навіть, найсучасніші аналітичні системи втрачають свою цінність без механізмів оперативного застосування результатів аналізу в реальному часі. Саме автоматизовані рішення сьогодні дозволяють державним

органам не лише швидше реагувати на інциденти, а й зменшувати залежність від людського фактору, який традиційно був слабкою ланкою системи інформаційної безпеки.

За останні роки у світі простежується чітка динаміка переходу від ручного контролю до комплексної автоматизації. За даними звіту *Gartner за 2024 рік*, понад 70 % державних органів країн-членів ЄС інтегрували автоматизовані SOC (Security Operations Center) рішення, які дозволяють скорочувати час реагування на кіберінциденти на 65–75 %. У США в межах програми *Continuous Diagnostics and Mitigation* автоматизовані інструменти охоплюють понад 80 % федеральних агентств і забезпечують щоденний моніторинг близько 9 мільйонів пристроїв. Це дозволило у 2024 році скоротити кількість успішних атак на федеральні установи на 18 % у порівнянні з попереднім роком.

В Україні ситуація виглядає дещо інакше. За даними Державної служби спеціального зв’язку та захисту інформації, у 2024 році лише близько 35 % органів державної влади використовували автоматизовані системи моніторингу подій безпеки (SIEM). Решта продовжує працювати за змішаними або переважно ручними схемами контролю. Це створює серйозний розрив між наявними загрозами та можливостями їх вчасного виявлення. У 2025 році цей показник дещо зріс завдяки впровадженню централізованої системи моніторингу при CERT-UA, проте частка охоплення все ще не перевищує 50 %.

Особливої уваги заслуговує фактор людського ресурсу. У 2024 році середній час реагування на кібератаку в українських держустановах становив 56 годин, тоді як автоматизовані системи в європейських країнах скорочують цей час до 6–10 годин. Різниця у понад п’ять разів свідчить про критичну необхідність інтеграції автоматизованих рішень, які здатні проводити цілодобовий моніторинг без перерви та відволікання.

Таблиця 4.3

Рівень автоматизації контролю та моніторингу інформаційної безпеки

Країна / Регіон	**Частка державних установ з автоматизованими системами (%)**	**Середній час реагування на інцидент**	**Динаміка у 2024–2025 рр.**
США	80 %	6–8 годин	+12 % охоплення
ЄС (середній показник)	70 %	8–10 годин	+9 % охоплення
Велика Британія	85 %	5–7 годин	+15 % охоплення
Україна	35 % (2024), 48 % (2025)	50–56 годин	+13 % охоплення
Польща	65 %	12–14 годин	+11 % охоплення

Ця статистика чітко показує, що відставання України у сфері автоматизації створює вразливість, яка у разі масштабних атак може мати катастрофічні наслідки для роботи органів державної влади. При цьому міжнародний досвід підтверджує: інвестиції у автоматизацію контролю й моніторингу швидко окуповуються, адже зменшення часу реагування напряму знижує фінансові збитки та втрати репутації. За оцінками *IBM Security (2024)*, середні збитки від витоку даних у держсекторі скорочуються з 4,9 млн дол. до 2,6 млн дол., якщо використовується автоматизований моніторинг та реагування.

Загалом, автоматизація процесів контролю та моніторингу інформаційної безпеки вже стала світовим трендом, а для України – це не питання вибору, а нагальна потреба. Реалізація масштабних проєктів у цій сфері здатна вивести національну систему кіберзахисту на якісно новий рівень, забезпечивши оперативність, ефективність і стійкість перед сучасними кіберзагрозами.

4.3. Формування культури інформаційної безпеки в державних установах

Система технічних та організаційних заходів у сфері інформаційної безпеки буде недостатньо ефективною, якщо працівники державних органів не матимуть належного рівня знань та навичок для їх правильного використання. Якраз людський фактор найчастіше стає причиною інцидентів, навіть за наявності сучасних технологій. За даними *Verizon Data Breach Investigations Report (2024)*, понад 74 % випадків витоку даних у державному секторі пов'язані з діями або помилками співробітників. Це означає, що формування сталої культури інформаційної безпеки починається з якісного навчання та регулярного підвищення кваліфікації.

В Україні система підготовки кадрів у цій сфері поки що має фрагментарний характер: тренінги проводяться переважно у вигляді коротких інструктажів, часто без практичної складової. За результатами опитування, проведеного Інститутом інформаційної безпеки у 2024 році, лише 28 % державних службовців проходили повноцінні курси з кібергігієни та захисту даних протягом останніх двох років, тоді як у країнах ЄС цей показник перевищує 60 %.

Для виправлення ситуації необхідно створити багаторівневу систему навчання, яка охоплюватиме як базову підготовку для всіх співробітників, так і спеціалізовані програми для керівників підрозділів та технічних спеціалістів.

По-перше, базові курси з кібергігієни повинні стати обов'язковими для кожного держслужбовця незалежно від посади. Такі програми мають охоплювати теми безпечного користування електронною поштою, виявлення фішингових атак, правил роботи з мобільними пристроями та дистанційними сервісами, захисту паролів і багатофакторної автентифікації. Навчання може здійснюватися у форматі щорічних онлайн-курсів із тестуванням, що дозволить автоматично підтверджувати рівень знань кожного співробітника.

По-друге, для керівників відділів та департаментів слід запровадити програми стратегічного рівня, орієнтовані на управління ризиками, кризове реагування та планування заходів кіберзахисту. Такі курси можуть проводитися у співпраці з провідними українськими університетами, Академією державного управління, а також міжнародними партнерами – наприклад, у межах програм НАТО з кіберстійкості.

По-третє, для технічних спеціалістів варто організувати спеціалізовані курси із сертифікацією за міжнародними стандартами (CISSP, CISM, CEH, CompTIA Security+). Це дозволить забезпечити відповідність українських кадрів світовим вимогам та підвищить рівень довіри до державних органів на міжнародній арені.

Практична користь таких програм підтверджується статистикою: у країнах Балтії, де з 2019 року діють обов'язкові тренінги з інформаційної безпеки для всіх держслужбовців, кількість успішних фішингових атак на державні органи знизилася на 37 % протягом трьох років. Водночас в Україні у 2024 році кількість виявлених випадків компрометації службових акаунтів зросла на 42 % у порівнянні з 2022 роком, що напряму свідчить про низький рівень підготовки персоналу.

Але, ефективність таких програм буде суттєво обмеженою без закріплення чітких стандартів кібергігієни, які мають бути обов'язковими для щоденного дотримання всіма працівниками державних органів. Інакше отримані знання залишаються лише теорією, не інтегрованою в реальну практику.

Кібергігієна — це не разові заходи, а система повсякденних правил і процедур, які зменшують ризик кіберінцидентів. У сучасних умовах, коли більшість державних установ активно переходять на цифрові сервіси, відсутність таких стандартів може призвести до критичних наслідків. Для прикладу, в 2024 році CERT-UA зафіксувала понад 18 тисяч фішингових кампаній, спрямованих на українські держоргани. При цьому близько 62 % випадків успішних атак стали можливими саме через нехтування базовими правилами кібергігієни з боку

співробітників: використання слабких паролів, нехтування двофакторною автентифікацією або відкриття шкідливих вкладень у пошті.

Запровадження стандартів має відбуватися на кількох рівнях. По-перше, на рівні індивідуальної відповідальності кожного співробітника, що включає регулярну зміну паролів, використання багатофакторної автентифікації, перевірку джерел електронних листів, заборону використання особистих носіїв у службових системах. По-друге, на рівні установи, де повинні бути чіткі регламенти роботи з інформацією, періодичне оновлення програмного забезпечення, контроль доступу до даних і аудит дотримання правил безпеки. Ну і, на рівні державної політики доцільно затвердити єдині міжвідомчі стандарти кібергігієни для всіх органів влади.

Досвід країн Балтії та Скандинавії доводить, що це не просто рекомендаційні практики, а реальний фактор підвищення кіберстійкості. У Литві, де ще у 2021 році було запроваджено обов'язковий «Кодекс кібергігієни» для держслужбовців, уже у 2024 році кількість випадків компрометації державних акаунтів знизилася майже на 40 %. У Швеції після впровадження аналогічних стандартів у рамках державної програми *Digital Resilience 2030* рівень фішингових інцидентів у держсекторі знизився на 32 % протягом двох років.

В Україні поки що такі стандарти не мають системного характеру. В різних відомствах практики відрізняються: наприклад, у Міністерстві фінансів вже з 2023 року діє внутрішній регламент кібергігієни, тоді як у багатьох обласних адміністраціях подібних документів немає. Це створює нерівномірність у рівні кіберзахисту, що робить слабші установи мішенню для атак і, відповідно, підриває захищеність усього державного сектору.

Загалом, розвиток трикутника «держава – бізнес – наука» здатен забезпечити комплексний підхід до кіберзахисту. Бізнес приносить технології та гнучкість, наука — інновації та нові кадри, а держава формує політичні рамки та забезпечує координацію. Взаємодія цих трьох складових створює середовище, де культура інформаційної безпеки перестає бути лише внутрішньою політикою

окремих органів влади і перетворюється на загальнонаціональний стандарт. Це є ключем до формування стійкої системи кіберзахисту, здатної протистояти викликам 2020-х років.

ВИСНОВКИ

У процесі дослідження ролі інформаційної безпеки в державному секторі було доведено, що вона є фундаментальною складовою національної безпеки, політичної стабільності та ефективності державного управління. Інформаційна безпека сьогодні виходить далеко за межі технічної проблематики: вона охоплює правові, організаційні, соціальні, кадрові та культурні аспекти, формуючи багаторівневу систему, від якої залежить життєздатність держави в умовах цифрової трансформації та глобальних викликів.

Проведений аналіз показав, що в Україні створено базове нормативно-правове підґрунтя для захисту інформації, яке відповідає міжнародним підходам. Закони «Про інформацію», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України» формують правові рамки функціонування системи безпеки. Однак, законодавча база характеризується фрагментарністю, недостатньою узгодженістю та надмірним акцентом на декларативних нормах при браку чітких механізмів практичної реалізації. Це обмежує ефективність державної політики та створює правові прогалини, якими користуються зловмисники.

Аналіз сучасних загроз показав, що державний сектор України перебуває під потужним впливом як зовнішніх, так і внутрішніх факторів ризику. Масові кібератаки на енергетичні компанії, державні реєстри, урядові сайти підтвердили вразливість критичної інфраструктури. Водночас, вагомими залишаються внутрішні проблеми: низький рівень кібергігієни, недостатня цифрова грамотність працівників, відсутність культури персональної відповідальності за захист даних. Статистичні дані засвідчують, що значна частка інцидентів виникає саме через людський фактор, а не лише через технічні вразливості.

Розгляд організаційно-правових механізмів виявив, що в Україні існує розгалужена система інституцій, відповідальних за інформаційну безпеку: РНБО, ДССЗЗІ, СБУ, Кіберполіція, Міністерство цифрової трансформації тощо. Проте між цими органами часто бракує належної координації, що призводить до

дублювання функцій або створення «білих плям» у зоні відповідальності. Це підтверджується аналізом інцидентів, коли через недостатню взаємодію державні органи реагували із затримкою, що збільшувало масштаби шкоди.

Практичні аспекти дослідження показали, що ефективність українських стратегій та програм кіберзахисту залишається обмеженою. Попри наявність державних ініціатив («Кібербезпека України», розвиток *Дія* та інші цифрові сервіси), їх впровадження нерідко наштовхується на проблеми недостатнього фінансування, застарілої технічної бази та нерівномірності у застосуванні між різними органами влади. Досвід міжнародних партнерів, зокрема країн Балтії та Скандинавії, доводить, що інтеграція стандартів кібергігієни, системний обмін інформацією між державою і бізнесом, а також масштабні програми навчання службовців суттєво знижують рівень вразливості державних систем.

В роботі було сформульовано низку практичних рекомендацій. По-перше, удосконалення законодавчої бази шляхом її систематизації та гармонізації з європейськими стандартами, особливо в частині захисту критичної інфраструктури та персональних даних. По-друге, розвиток інноваційних технологій захисту, зокрема впровадження блокчейн-рішень у державних реєстрах, використання Big Data та штучного інтелекту для аналізу загроз, а також автоматизації процесів моніторингу. По-третє, формування сталої культури інформаційної безпеки через обов’язкові програми навчання держслужбовців, запровадження єдиних стандартів кібергігієни та розвиток тристоронньої співпраці між державою, бізнесом і науковими установами.

Загалом, результати дослідження підтверджують, що інформаційна безпека є не лише технічним завданням, а системоутворюючим чинником сучасної держави. Вона визначає здатність державного сектору ефективно виконувати свої функції, зберігати стабільність у кризових ситуаціях, протидіяти зовнішнім агресіям і гарантувати довіру громадян до цифрових сервісів. Для України в умовах гібридних загроз і війни інформаційна безпека є питанням виживання та поступального розвитку. Тому державна політика у цій сфері має спиратися на комплексний підхід, що поєднує правові, технологічні,

організаційні та культурні аспекти, забезпечуючи стійкість національної інформаційної інфраструктури у довгостроковій перспективі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Поняття інформаційної безпеки. URL: https://studfile.net/preview/6012701/
2. Олійник О.В. Принципи забезпечення інформаційної безпеки України. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/1be420c6-c827-4c42-b061-af13d6ba118f/content
3. Боднар І.Р. Інформаційна безпека як основа національної безпеки. URL: https://files.core.ac.uk/download/pdf/141443493.pdf
4. Інформаційна безпека: що це і навіщо вона потрібна. URL: https://vgoru.org/cikavo/informaciina-bezpeka-shho-ce-i-navishho-vona-potribna?gad_source=1&gad_campaignid=23005040121&gbraid=0AAAABAp6m8uiGgBg2XysiIMmgqAersZ65&gclid=Cj0KCQiA5abIBhCaARIsAM3-zFWu-gA2vBkYEXEjYwwCFsfyLbSuT5as85xbrxIuzVK5NYlPsvKSspAaAkZrEALw_wcB
5. Нормативно-правова база забезпечення інформаційної безпеки України: сучасні проблеми та відправні точки їх вирішення. URL: https://ippi.org.ua/sites/default/files/14_17.pdf
6. Концепція інформаційної безпеки України. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf
7. Правове забезпечення інформаційної безпеки при побудові інформаційного суспільства в Україні. URL: https://dspace.wunu.edu.ua/bitstream/316497/46756/1/%D0%9A%D1%83%D1%80%D0%B8%D0%BB%D0%BE%D0%94.%D0%92..pdf
8. Цибульник Н.Ю. Інформаційно-правова характеристика основних складових сектору безпеки держави. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/01/95.pdf
9. Шевчук М.О. Сучасні виклики і загрози в сфері інформаційної безпеки держави. URL: http://apnl.dnu.in.ua/6_2024/27.pdf
10. Ткаченко В.В. Загрози інформаційній безпеці України як проблематика національної безпеки. URL: http://lsej.org.ua/10_2022/123.pdf

11. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2019. № 9. С. 100-108.
12. Боднар, І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія/ І. Р. Боднар. – Львів : Видавництво Львівської комерційної академії, 2013. – 320 с.
13. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. Київ : ТОВ «СІК ГРУП Україна», 2015. 449 с.
14. Виздрик В., Мельник О. Інформаційна безпека в Україні. Grail of Science. 2023. № 24. С. 196–202.
15. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203
16. Герасименко І. О. Основні загрози та виклики інформаційній безпеці в державному секторі. Сучасні наукові тенденції в роботах молодих вчених : матеріали ІІІ. наук-практ. конф. (м. Київ, 25 квіт. 2025 р.). Київ : Київський інститут НГУ, 2025. С. 47–50.
17. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки. Юридичний часопис НАВС. 2018. № 1. С. 141–153.
18. Дудикевич В.Б., Опірський І.Р., Гаранюк П.І., Зачепило В.С., Партика А.І. Забезпечення інфор- маційної безпеки держави : навчальний посібник. Львів : Видавництво Львівської політехніки, 2017. 204 с.
19. Залєвська І.І., Удренас Г.І. Інформаційна безпека в Україні в умовах російської військової агресії. Південноукраїнський правничий часопис. 2022. № 1. С. 20–26.
20. Зозуля О.С. Періодизація розбудови системи державного управління забезпеченням інформаційної безпеки України. Інвестиції: практика та досвід. Київ, 2016. № 8. С. 106–114.

21. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. 2019. № 1. Вип. 2. С. 27–32.
22. Інформаційна безпека держави : підручник: в 2 т. Т. 1. / В.М. Петрик та ін. ; за заг. ред. В.В. Остроухова. Київ : ДНУ «Книжкова палата України», 2016. 264 с.
23. Камінська Н.В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. Міжнародне право: виклики сьогодення : матер. Міжнар. науково-практ. конф. (Київ, 20 грудня 2016 р.) Київ, 2016. С. 22–27.
24. Колпаков В. К. Адміністративне право України: Підручник / В. К. Колпаков, О. В. Кузьменко. – К.: Юрінком Інтер. – 2003. – 544 с.
25. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України. Системи обробки інформації. 2016. Вип. 8 (145). С. 115–117.
26. Лісовська Ю.П. Інформаційна безпека України : навчальний посібник. Київ : Кондор, 2018. 172 с.
27. Мануйлов Є.М., Калиновський Ю.Ю. Аксіологічний вимір інформаційної безпеки української держави. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». № 3 (34) 2017. С. 13-30.
28. Методичні вказівки до практичних занять з навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» / уклад.: Л.В. Перевалова, І.В. Лисенко, Г. М. Гаряєва. – Харків: НТУ «ХПІ», 2023. – 68 с.
29. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2018. № 1. С. 17–23.
30. Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві: навч.-метод. посіб. / Л. В. Перевалова, І. В. Лисенко, А.М. Лисенко, Г. М. Гаряєва – Харків: НТУ «ХПІ», 2023. – 110 с.

31. Панченко О. Інформаційна безпека держави як елемент соціокультури. Аспекти публічного управління. 2020. № 1. С. 58–67.
32. Перун Т. Значення адміністративної відповідальності в системі заходів забезпечення інформаційної безпеки. Право України. 2017. № 10. С. 202-209.
33. Платоненко А.В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. Сучасний захист інформації. 2015. № 4. С. 86–90.
34. Почепцов, Г. Інформаційна політика: навч. посібник [Текст] / Г. Г. Почепцов. – К.: Знання, 2006. – 663 с.
35. Правові засади управлінської діяльності: навч.-метод. посіб. / Л.В. Перевалова, О.В. Гаєвая, Г.М. Гаряєва, І.В. Лисенко. Харків : ФОП Панов А.М., 2020. - 50 с.
36. Семенець-Орлова І.А. Державне управління освітніми змінами в Україні: теоретичні засади : монографія. Київ : ЮСТОН, 2018. 420 с.
37. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с.
38. Уханова Н.С. Правова культура молоді в Україні. Інформація і право. 2019. № 2. С. 156–166.
39. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: Глосарій / за заг. ред. Р.А. Калюжного. Київ: Текст, 2004. 180 с.
40. Чмир Я.І. Проблеми забезпечення інформаційної безпеки у системі публічного управління. Аспекти публічного правління. Том 6. № 9. 2018.
41. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2019. Том 30 (69). № 4. С. 31–37.