МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет економіки та управління

Кафедра національної економіки та публічного управління

Освітньо-професійна програма:
Державна політика та публічне управління
Галузь знань: 28 Публічне управління та адміністрування
Спеціальність: 281 Публічне управління та адміністрування

Форма здобуття освіти: очна (денна)

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему «**Цифрові інструменти кіберзахисту державних інформаційних ресурсів»**

здобувача Пономаренка Ярослава Олександровича

Науковий керівник: ***д. філософ. п.у.а Осьмак Антон Сергійович***

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: ***д.держ.упр., професор Карпенко О.В.***

_____

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет економіки та управління

Кафедра національної економіки та публічного управління

Освітньо-професійна програма:
Державна політика та публічне управління
Галузь знань: 28 Публічне управління та адміністрування
Спеціальність: 281 Публічне управління та адміністрування

ПОГОДЖЕНО
Керівник проєктної групи (гарант)
освітньо-професійної програми
А.С. Осьмак
_____ 2024 р.

ЗАТВЕРДЖУЮ
Завідувач кафедри
О.В.Карпенко
_____ 2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Пономаренку Ярославу Олександровичу

очної (денної) форми здобуття освіти

на підготовку кваліфікаційної магістерської роботи

на тему **«Цифрові інструменти кіберзахисту державних інформаційних ресурсів»**

Тему затверджено наказом ректора Університету від «27» вересня 2024 р. № 1686-ст

Кваліфікаційна магістерська робота виконується на матеріалах Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України.

План кваліфікаційної магістерської роботи

Розділ 1	Теоретичні засади кіберзахисту державних інформаційних ресурсів

Розділ 2	Практика кіберзахисту державних інформаційних ресурсів в Україні

Розділ 3	Удосконалення кіберзахисту державних інформаційних ресурсів

Об'єкт дослідження:	Кіберзахист державних інформаційних ресурсів в Україні
Предмет дослідження:	Цифрові інструменти кіберзахисту державних інформаційних ресурсів
Мета кваліфікаційної магістерської роботи:	Дослідити теоретико-методичні основи цифрових інструментів кіберзахисту державних інформаційних ресурсів

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	− Розкрити поняття державних електронних інформаційних ресурсів; − Визначити сутність та роль кіберзахисту державних інформаційних ресурсів; − Провести огляд класифікації цифрових інструментів кіберзахисту державних інформаційних ресурсів.
У розділі 2	− Дослідити нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів; − Розглянути систему національної безпеки в кібереконом ічному просторі; − Дослідити стан розвитку кібербезпеки України.
У розділі 3	− Розробити напрями вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації; − Запропонувати перспективи розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів.

Завдання підготував науковий керівник _____ А.С. Осьмак

«29» вересня 2024 р.

Завдання одержав здобувач _____ Я.О. Пономаренко

«29» вересня 2024 р.

Реферат

Кваліфікаційна магістерська робота містить 88 сторінок, 11 рисунків, список використаних джерел з 97 найменувань.

«Цифрові інструменти кіберзахисту державних інформаційних ресурсів»

Об'єктом дослідження є кіберзахист державних інформаційних ресурсів в Україні.

Предметом дослідження є цифрові інструменти кіберзахисту державних інформаційних ресурсів.

Мета і завдання дослідження. Дослідити теоретико-методичні основи цифрових інструментів кіберзахисту державних інформаційних ресурсів.

Відповідно до поставленої мети визначені такі *завдання*:

- Розкрити поняття державних електронних інформаційних ресурсів;
- Визначити сутність та роль кіберзахисту державних інформаційних ресурсів;
- Провести огляд класифікації цифрових інструментів кіберзахисту державних інформаційних ресурсів;
- Дослідити нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів;
- Розглянути систему національної безпеки в кібереконо мічному просторі;

- дослідити стан розвитку кібербезпеки України;

- Дослідити стан розвитку кібербезпеки України;
- Вивчити світовий досвід забезпечення інформаційної безпеки держави;
- Розробити напрями вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації;
- Запропонувати перспективи розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів.

Теоретична, методична значущість отриманих результатів полягає у дослідженні теоретичних засад кіберзахисту державних інформаційних ресурсів та їх впливу на діяльність системи публічного управління.

Практичне значення отриманих результатів полягає в проведені дослідження розвитку кібербезпеки України та розробці рекомендацій щодо розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів.

Описані пропозиції можуть використовуватися органами публічної влади при формуванні політики у сферах кібербезпеки та цифрових трансформацій, сприяти у визначенні пріоритетних напрямів розвитку кібербезпеки у діяльності держави.

Рік виконання кваліфікаційної магістерської роботи – 2024.

Рік захисту роботи – 2024.

Ключові слова: «державне управління», «кібербезпека», «публічне управління», «кіберзахист», «інформаційні ресурси», «цифрові інновації», «цифрові трансформації».

ВІДГУК

про кваліфікаційну магістерську роботу
здобувача факультету економіки та управління
освітньо-професійної програми **«Цифрове врядування»**
Пономаренка Ярослава Олександровича
на тему «Цифрові інструменти кіберзахисту державних інформаційних ресурсів»

1. Актуальність теми зумовлена необхідністю вдосконалення цифрових інструментів кіберзахисту державних інформаційних ресурсів є надзвичайно аважливим в умовах стрімкого зростання кіберзагроз і дедалі складніших методів кібератак.

2. Позитивні риси кваліфікаційної магістерської роботи. Дослідження характеризується високим рівнем наукової обґрунтованості та комплексним підходом до аналізу зазначеної проблематики. У роботі успішно вирішено низку важливих наукових завдань, зокрема, розкрито поняття державних електронних інформаційних ресурсів; проведено огляд класифікації цифрових інструментів кіберзахисту державних інформаційних ресурсів; досліджено нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів.

3. Наявність самостійних розробок автора. У дослідженні представлено авторські розробки та здійснено аналіз світового досвіду у сфері кіберзахисту державних інформаційних ресурсів. Особливу увагу приділено перспективі розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів.

4. Цінність теоретичних висновків та практичних рекомендацій. Теоретичні висновки дослідження дозволяють більш широко розглянути процеси в межах системи реагування на існуючі загрози, забезпечення громадського інформаційного простору, організації та роботи спеціалізованих інституцій щодо захисту національних інтересів в інформаційній сфері. Надано практичні рекомендації щодо шляхів інтеграції міжнародного досвіду в забезпечення інформаційної безпеки в Україні.

5. Наявність недоліків. Недоліком даного дослідження є недостатньо цілісність викладу інформації та незначні вади в оформленні роботи. Водночас цей аспект не знижує загальної наукової цінності та якості проведеного дослідження.

6. Загальна оцінка кваліфікаційної магістерської роботи та її допущення до захисту перед ЕК: Кваліфікаційна магістерська робота Пономаренка Ярослава Олександровича виконана на професійному рівні, результати дослідження дають відповідь на поставлені завдання у вступі, робота відповідає всім наявним вимогам та може бути допущена до захисту з оцінкою «відмінно».

Науковий керівник: *д. філос. з публічного управління та адміністрування*

«___» _____ 2024 р. _____ *Осьмак Антон Сергійович*

РЕЦЕНЗІЯ
на кваліфікаційну магістерську роботу
Пономаренко Ярослава Олександровича
«Цифрові інструменти кіберзахисту державних інформаційних ресурсів»

Кваліфікаційна робота Пономаренко Я.О. розкриває результати дослідження актуальної проблеми кіберзахисту державних інформаційних ресурсів. Враховуючи стрімке зростання кіберзагроз, надзвичайно важливо використовувати цифрові інструменти для кіберзахисту державних інформаційних ресурсів. Урядові інформаційні системи містять конфіденційні дані, такі як особиста, фінансова та стратегічна інформація, що робить їх вразливими для хакерських і шпигунських атак, особливо в умовах війни. Забезпечення національної безпеки та стабільного функціонування державних інституцій вимагає вдосконалення методів захисту даних ресурсів.

Кваліфікаційна робота виконана на достатньому теоретичному та методичному рівні. Вона містить вступ, три розділи, список використаних джерел, додатки. Відповідно до теми сформульовано методологічний апарат: мету, завдання, об’єкт, предмет.

В результаті проведеної дослідницької роботи визначено основні термінологічні засади державних електронних інформаційних ресурсів, розкрито значення кіберзахисту державних інформаційних ресурсів, окреслено їх класифікацію.

Автором здійснено спробу дослідити нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів та їх практичне застосування в межах кіберекономічного простору. Визначено основні напрями сучасної роботи системи кібербезпеки України та її перспективи розвитку.

Цінністю роботи виступають рекомендації, розроблені на основі аналізу міжнародного досвіду та роботи сучасних цифрових інструментів для забезпечення інформаційної безпеки та організації доступу до публічної інформації, що складає практичне значення результатів дослідження.

Кваліфікаційна робота Пономаренко Я.О. «Цифрові інструменти кіберзахисту державних інформаційних ресурсів» є самостійним завершеним дослідженням, виконана з дотриманням всіх вимог і заслуговує на позитивну оцінку за умови успішного захисту.

Рецензент:
Заступник голови ГО «Цифрове врядування» Петро ШПИГА

ЗМІСТ

ВСТУП

Актуальність теми. Використання цифрових інструментів кіберзахисту державних інформаційних ресурсів є надзвичайно важливим в умовах стрімкого зростання кіберзагроз і дедалі складніших методів кібератак. Інформаційні системи державного рівня містять критично важливі дані, зокрема персональну, фінансову та стратегічну інформацію, що робить їх особливо вразливими для атак хакерів і шпигунських програм. Удосконалення методів захисту таких ресурсів є необхідним для забезпечення національної безпеки та стабільного функціонування урядових структур. Сучасні цифрові інструменти кіберзахисту, як-от антивірусні системи, сканери вразливостей і аналізатори мережевого трафіку, дозволяють забезпечити комплексний захист інформаційної інфраструктури. Впровадження інноваційних рішень у сфері кібербезпеки стає пріоритетним завданням для держав, оскільки воно допомагає попереджати можливі атаки та оперативно реагувати на загрози.

Аналіз останніх досліджень і публікацій. Дослідженню теоретичних та практичних засад цифрових інструментів кіберзахисту державних інформаційних ресурсів присвячені праці Арсенович Л.А., Блінова Г., Білик О., Євсюкова О.В., Київська К.І., Кисленко Д.П., Кіндзерський Ю.В., Корніленко О., Олексюк Л., Стендер С.В, Снітко Ю.М., Столбовий В.М., Тарасюк А.В., Терентьєв О.О., Фротер О.С., Цюцюра С. В., та інших

Мета і завдання дослідження. Мета кваліфікаційної магістерської роботи дослідити теоретико-методичні основи цифрових інструментів кіберзахисту державних інформаційних ресурсів.

В дослідженні були визначені такі *завдання*:

– розкрити поняття державних електронних інформаційних ресурсів;

– визначити сутність та роль кіберзахисту державних інформаційних ресурсів;

– провести огляд класифікації цифрових інструментів кіберзахисту державних інформаційних ресурсів;

– дослідити нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів;

– розглянути систему національної безпеки в кібереконо мічному просторі;

– дослідити стан розвитку кібербезпеки України;

– вивчити світовий досвід забезпечення інформаційної безпеки держави;

– розробити напрями вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації;

– запропонувати перспективи розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів.

Об'єктом дослідження є кіберзахист державних інформаційних ресурсів в Україні.

Предметом дослідження є цифрові інструменти кіберзахисту державних інформаційних ресурсів.

Методи дослідження: аналізу та синтезу, порівняння, систематизації та узагальнення, описовий, спостереження, контент-аналіз, метод графічного представлення даних.

Теоретична, методична значущість отриманих результатів полягає у дослідженні теоретичних засад цифрових інструментів кіберзахисту державних інформаційних ресурсів та визначенні основних напрямів удосконалення системи кіберзахисту інформаційних ресурсів

Практична значущість отриманих результатів полягає в проведені дослідження розвитку кібербезпеки України та розробці рекомендацій щодо розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів.

Інформаційна база дослідження стали нормативно-правові акти щодо регулювання кіберзахисту державних інформаційних ресурсів в Україні, наукові статті, Інтернет-джерела, фахові публікації, статистичні дані, звіти та аналітичні матеріали на тему дослідження.

Перший розділ: В першому розділі розглянуто основні теоретичні засади кіберзахисту державних інформаційних ресурсів, окреслено основну термінологію, сутність та значення захисту національних інформаційних ресурсів в системі державного управління, наведено класифікацію цифрових інструментів кіберзахисту державних інформаційних ресурсів.

Другий розділ: В другому розділі визначено особливості забезпечення національної інформаційної безпеки в Україні, окреслено нормативно-правові засади, що забезпечують основу інформаційного захисту на державному рівні, проаналізовано основні засади функціонування системи в кіберекономічному секторі та сучасний стан розвитку системи інформаційного захисту.

Третій розділ: В третьому розділі здійснено аналіз основних напрямів вдосконалення системи державних інформаційних ресурсів, визначено основні засади забезпечення інформаційної безпеки держави відповідно до міжнародного досвіду, наведено перспективи розвитку системи кіберзахисту, враховуючи застосування сучасних технологій.

Структура роботи: Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Апробація матеріалів кваліфікаційної магістерської роботи: Участь у роботі 91-і щорічної студентської наукової конференції «ІННОВАЦІЙНІ ПРОЄКТИ ДЛЯ ЕКОНОМІЧНОГО ВІДРОДЖЕННЯ ТА КОНКУРЕНТНОГО РОЗВИТКУ УКРАЇНИ» з публікацією тез доповіді на тему «Особливості забезпечення кіберзахисту державних інформаційних систем в умовах кризових викликів сьогодення».

Пономаренко Я.О. Особливості забезпечення кіберзахисту державних інформаційних систем в умовах кризових викликів сьогодення. *Інноваційні проєкти для економічного відродження та конкурентного розвитку України* : зб. доп. 91-і щорічної студентської наукової конференції, 15 квітня – 19 травня 2024 р. [Електронний ресурс]. Київ : КНЕУ, 2024. С. 92-94.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Поняття державних електронних інформаційних ресурсів

Ефективне використання інструментів цифрової економіки є суттєвим елементом інтеграції державних електронних інформаційних ресурсів, що сприятиме підвищенню якості державного управління, зниженню витрат на обслуговування численних реєстрів та покращенню статистичного контролю. Проте, наразі в Україні існує надмірна кількість державних органів, що утримують окремі електронні реєстри, що створює фінансове навантаження на державний бюджет, особливо в умовах поточних викликів. Бюджетні витрати постійно зростають, проте їхній вплив на економічні процеси залишається малопомітним. Для побудови ефективних електронно-інформаційних ресурсів слід почати з нормативно-правового врегулювання, враховуючи ідеологічні, технологічні та управлінські аспекти національної економіки [1].

Розглянемо законодавчі та наукові підходи до поняття «інформаційні ресурси». Відповідно до Закону України «Про Національну програму інформатизації», інформаційний ресурс визначається як сукупність документів, що містяться в інформаційних системах, таких як бібліотеки, архіви, банки даних тощо. Хоча законодавець не зазначає конкретно електронну форму документів, з огляду на мету цього закону є задоволення інформаційних потреб громадян і суспільства шляхом розвитку інформаційних систем, мереж, ресурсів і технологій на основі сучасних комп’ютерних і комунікаційних систем створення умов для їх виконання – можна стверджувати, що йдеться саме про електронні інформаційні ресурси [2].

Основою для розвитку цифрової економіки в Україні стала прийнята Концепція розвитку цифрової економіки та суспільства на 2018–2020 рр. [3], адже нині цифрова економіка виступає ефективною платформою для зміцнення державного управління, забезпечення незалежності та національної безпеки. Після зосередження уваги держави на процесі цифровізації та запуску відповідної програми в Україні було створено й успішно функціонує низка цифрових платформ для онлайн-державних послуг. Водночас Україні бракує збалансованого підходу до розвитку державних електронних ресурсів (ДЕІР). Систематичне впровадження такого підходу здатне підвищити громадський контроль за соціальними виплатами, зменшити рівень шахрайства, сприяти промисловому розвитку, стимулювати інновації, розвивати ІТ-інфраструктуру, забезпечити стабільне економічне зростання, знизити безробіття та бідність, а також покращити освітні та медичні послуги [1].

У березні 2014 року в українське законодавство було введено таке визначення поняття «державні інформаційні ресурси»: «...це інформація, яка перебуває в розпорядженні державних органів, військових формувань, а також інформація, створення якої передбачено законодавством і яка обробляється фізичними чи юридичними особами відповідно до повноважень, наданих їм суб'єктами владних повноважень» [4]. У наведеному визначенні основний акцент робиться на тому, що державні органи є власниками цієї інформації, а її обробка може здійснюватися фізичними чи юридичними особами за дорученням. Однак в розкритому вище терміні не окреслено зміст прав державних органів щодо використання та розпорядження цією інформацією, а також не уточнено питання систематизації даних і їх зв'язку з інформаційними технологіями.

Однією з ключових проблем є відсутність термінологічної узгодженості у різних нормативно-правових актах, що регулюють роботу та використання державних електронних інформаційних ресурсів задля забезпечення ефективної інформаційної безпеки. Українське законодавство використовує ряд термінів для позначення різних типів таких ресурсів, серед яких: «автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання», «автоматизована

інформаційно-телекомунікаційна система», «база даних», «електронна інформаційно-телекомунікаційна система», «геоінформаційна система», «державний реєстр», «портал електронних сервісів», «програмно-інформаційний комплекс», «інформаційна (автоматизована) система», «організаційно-технічна система», «багатофункціональна інтегрована автоматизована система», «єдиний державний реєстр», «вебпортал» тощо. Така термінологічна різноманітність свідчить про відсутність єдиної методологічної основи для визначення змісту, структури та критеріїв систематизації державних електронних інформаційних ресурсів [5].

Безумовно, електронні державні послуги не повинні спиратися на наявні бізнес-процеси та паперові взаємодії між органами влади, оскільки такі послуги, навіть після переведення в електронний формат, залишаються забюрократизованими та підверненими корупційним ризикам. Послуги нового типу слід розробляти виключно з використанням електронних взаємодій з державними реєстрами, а також прагнути до максимальної автоматизації процесів ухвалення рішень, щоб зменшити вплив людського чинника.

На жаль, нинішня відсутність ефективної взаємодії між державними реєстрами призводить до того, що громадянам та представникам юридичних осіб доводиться багаторазово відвідувати численні державні установи для отримання необхідних довідок. Це не лише викликає додаткові матеріальні та часові витрати, а й створює умови для розвитку низової корупції.

У 2016 році в Україні була схвалена Концепція розвитку електронних послуг, що передбачала переведення 45 ключових послуг у електронний формат протягом трьох років. Для забезпечення ефективної електронної взаємодії між державними органами було розроблено Постанову № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів», прийняту 8 вересня 2016 року. Цією постановою затверджено «Положення про електронну взаємодію державних електронних ресурсів» та визначено 15 пріоритетних національних електронних інформаційних ресурсів, які потребують інтеграції в систему електронної взаємодії для забезпечення безперебійного обміну

інформацією між державними установами та громадськістю [**Error! Reference source not found.**].

Переважна кількість запитів під час надання державних послуг зазвичай адресована саме до таких державних реєстрів (рис. 1.1)

Рисунок 1.1 – Найбільш затребувані державні реєстри

Джерело: складено автором на основі [6]

Уряд України ухвалив постанову «Про деякі питання електронної взаємодії державних електронних інформаційних ресурсів», що передбачає створення системи електронної інтеграції державних інформаційних ресурсів відповідно до стандартів ЄС.

Положення про електронну взаємодію державних інформаційних ресурсів встановлює основні принципи обміну електронними даними між суб'єктами владних повноважень, за винятком інформації, що має статус державної таємниці. Цей обмін здійснюється в рамках надання адміністративних послуг та виконання інших покладених функцій. Система електронної взаємодії спрямована на автоматизацію і технічну підтримку передачі електронних даних між державними органами через сервіс-орієнтовану архітектуру, що використовує стандартизовані

API, формати, протоколи, довідники, шаблони та класифікатори відповідно до єдиних вимог.

Механізм організації електронної інформаційної взаємодії державних інформаційних ресурсів визначається порядком, що встановлює правила інтеграції електронних даних між державними ресурсами. Для цього суб’єкти владних повноважень використовують програмне забезпечення Національного реєстру електронних ресурсів. Державне агентство з питань електронного урядування за допомогою цього комплексу створює особисті кабінети для суб’єктів владних повноважень, де розміщуються форми для заявок постачальників та одержувачів даних [7].

Національний реєстр електронних інформаційних ресурсів створений для впровадження єдиної системи обліку державних електронних ресурсів, використовуючи передові інформаційно-телекомунікаційні технології. Він являє собою систему для реєстрації, обліку, накопичення, обробки та зберігання інформації про структуру, зміст, розташування і доступ до електронних ресурсів, щоб забезпечити інформаційні потреби юридичних та фізичних осіб. До реєстру включено дані про державні електронні реєстри, кадастри, обов'язкові класифікатори, а також системи, що їх підтримують та використовують їхні дані. Відповідальність за реєстр покладена на Державне агентство з питань електронного урядування, яке фінансує його розробку та обслуговування за кошти державного бюджету. Державні органи та установи публічного права мають безкоштовний доступ до інформаційних ресурсів реєстру [5].

Положення про електронну взаємодію державних інформаційних ресурсів визначає перелік пріоритетних електронних ресурсів, обов’язкових для реєстрації в Національному реєстрі. Серед важливих державних електронних реєстрів України, що сприяють ефективній електронній взаємодії, можна зазначити такі системи, як реєстр юридичних осіб, фізичних осіб-підприємців і громадських об'єднань, реєстр прав на нерухоме майно, а також реєстраційні системи актів цивільного стану і довіреностей. До цього списку також входять реєстри, що містять інформацію про обтяження рухомого майна та земельний кадастр. Окрім

того, важливу роль відіграють демографічні реєстри, реєстри платників податків та ПДВ, а також система, що враховує осіб з правом на пільги. Не менш важливими є інформаційні системи Міністерства внутрішніх справ, включаючи реєстр транспортних засобів, реєстр соціального страхування, реєстрація виборців, а також судові реєстри та документи щодо будівельних робіт. Крім того, електронні платформи охорони здоров'я та освіти теж є ключовими елементами інтегрованої державної інформаційної системи.

Створення і функціонування вказаних державних електронних інформаційних ресурсів регламентується такими категоріями нормативно-правових документів (рис. 1.2).

Рисунок 1.2 – Регулятори функціонування державних електронних інформаційних ресурсів

Джерело: [5]

Класифікація державних електронних інформаційних ресурсів відбувається за такими критеріями: сфера застосування; власник реєстру; адміністратор реєстру; основні користувачі реєстру; строк дії реєстру; доступ до інформації в реєстрі; права власності на реєстр; територія використання; обсяг інформації, що міститься; рівень систематизації даних; порядок та спосіб доступу до інформації; платність

або безкоштовність доступу; правовий статус, який регулює реєстр; призначення реєстру; складність структури; кількість державних установ, що користуються даними.

Класифікація за цими характеристиками повинна визначати специфічні принципи функціонування кожної групи ресурсів [5].

Оскільки державні електронні інформаційні ресурси створюються на основі законодавства та фінансуються з держбюджету, їх створення, використання та захист потребують правового регулювання. У сфері державного управління дослідники зауважують, що поряд із цими ресурсами регулюються й інформаційні та комунікаційні системи, які належать державним і комунальним установам, органам місцевого самоврядування, а також надаються електронні адміністративні послуги. Важливою особливістю державних інформаційних ресурсів є те, що вони підпорядковуються правовим нормам, які визначають порядок їх функціонування.

Отже, державні електронні інформаційні ресурси відіграють ключову роль у модернізації державного управління в Україні, забезпечуючи ефективну інтеграцію інформації та автоматизацію процесів. Незважаючи на значні досягнення в розвитку цифрових платформ та електронних послуг, існує необхідність у нормативно-правовому регулюванні, яке визначатиме структуру, зміст і критерії систематизації таких ресурсів. Важливою проблемою залишається термінологічна несумісність у різних законодавчих актах, що ускладнює їхнє використання та взаємодію. Крім того, для досягнення максимальної ефективності державних електронних послуг важливо переходити від паперових форм до повністю автоматизованих електронних взаємодій, що зменшить бюрократичні перепони та корупційні ризики. У цілому, розвиток та вдосконалення державних електронних інформаційних ресурсів є невід'ємною частиною сучасної цифрової економіки та сприяє забезпеченню прозорості і доступності адміністративних послуг для громадян.

1.2 Сутність та роль кіберзахисту державних інформаційних ресурсів

Останнім часом суспільство все частіше зіштовхується з різними видами кіберзагроз, що впливають на роботу державних органів та приватного сектору. Серед них – збої в наданні електронних послуг, що блокують функціонування державного забезпечення, фішингові атаки, порушення конфіденційності та цілісності даних, а також інформаційно-психологічний тиск на населення, кібершпигунство та кібертероризм. Крім того, значні ризики створює інформаційне проникнення в національний інформаційний простір, що загрожує безпеці стратегічних об'єктів і приватної економіки. Україна стоїть перед необхідністю рішучих і термінових заходів у сфері кібербезпеки, адже останні кібератаки на критичну інфраструктуру, такі як NotPetya, підтверджують її вразливість. Для посилення захисту держави необхідно ідентифікувати основні проблеми у сфері кібербезпеки та шляхи їх вирішення [8].

Сьогодні кіберпростір набув статусу однієї з найважливіших складових інформаційного середовища, перетворившись на арену сучасних війн у віртуальному вимірі. Враховуючи дані особливості, кібербезпека виступає ключовим інструментом регулювання кіберпростору, водночас виступаючи важливим елементом системи національної безпеки держави [9].

Забезпечення кібербезпеки покладає на державу юридичну, організаційну та політичну відповідальність. Зважаючи на те, що захист критично важливої інформації та інфраструктури є базисом безпеки та стабільного розвитку держави, заходи з кіберзахисту мають ініціюватися та координуватися на найвищому рівні державної влади.

У широкому розумінні кібербезпека визначається як стан захищеності інформаційного середовища, який забезпечує дотримання прав та законних інтересів особи, суспільства і держави в інформаційній сфері [10].

Кібербезпека може бути визначена через такі ключові аспекти (рис.1.3).

Виходячи з вищезазначеного, кібербезпека є фундаментом національної безпеки України. Дана система забезпечує стан захищеності держави, суспільства та системи публічного управління у кіберпросторі завдяки впровадженню ефективних засобів забезпечення кіберзахисту в межах публічного управління.

Забезпечення інформаційної безпеки держави є одним із ключових чинників, який визначає стабільність та розвиток економічної, військової і політичної сфер. У сучасних умовах глобалізації та активного впровадження цифрових технологій інформаційні атаки стали потужним інструментом впливу на державні інституції, суспільство та економічні процеси [11].

Одними з найбільш ефективних методів інформаційного впливу є: залякування, глузування, схематизм, квлинювання, дезінформація та фальшування.

Рисунок 1.3 – Ключові характеристики кібербезпеки

Джерело: [10]

Дезінформація, як один із найбільш поширених методів, використовується для формування хибного уявлення про події або явища з метою маніпулювання рішеннями та поведінкою противника чи цільових груп. Наприклад, дезінформація може бути спрямована на підрив довіри до державних інституцій, дискредитацію військових або політичних лідерів, а також створення економічної нестабільності шляхом маніпуляцій на фінансових ринках [12].

Таким чином, ефективна протидія інформаційним атакам вимагає комплексного підходу, що включає технічні, правові та організаційні заходи, зокрема розвиток інформаційної грамотності населення, впровадження сучасних технологій кіберзахисту та активізацію міжнародного співробітництва у сфері інформаційної безпеки.

Обсяг інформаційних ресурсів постійно зростає, а кількість користувачів, які взаємодіють та працюють без географічних меж, неухильно збільшується. У відповідь на це кіберзлочинці застосовують складні методи для отримання несанкціонованого доступу до ресурсів, викрадення конфіденційних даних і саботажу діяльності компаній з метою вимагання фінансової вигоди.

Основними об’єктами кібератак є:

1. Діяльність уряду, збройних сил та правоохоронних органів – комунікаційні системи державної, комунальної та інших форм власності, які використовуються для обробки інформаційних ресурсів і обслуговують органи державної влади, правоохоронні структури та військові формування.

2. Ядерна та хімічна промисловість – інформаційні системи об’єктів критичної інфраструктури, до яких належать українські атомні електростанції (АЕС) та національні хімічні підприємства.

3. Транспортні та комунікаційні мережі – системи, що забезпечують суспільні потреби та функціонування електронного документообігу, електронної комерції, державних послуг тощо.

4. Національна та фінансова системи – комунікаційні мережі фінансових установ, серед яких окремо виділяються банківські системи, які є критично важливими для економічної стабільності країни [13].

Ці об’єкти становлять пріоритетні цілі для зловмисників через їх стратегічне значення для безпеки, економіки та функціонування держави.

Кіберпростір розглядається як середовище, у якому можливе здійснення злочинних дій, зокрема несанкціонованого доступу до конфіденційної інформації, порушення роботи програмного забезпечення та збоїв у функціонуванні автоматизованих систем. Сучасні реалії свідчать про значне зростання кількості кіберінцидентів та атак на державні інформаційні ресурси і об'єкти критичної інфраструктури України, що ставить під загрозу національну безпеку та стабільність ключових секторів країни [14].

Глобальний та всеосяжний характер кіберпростору суттєво ускладнює процес ідентифікації кіберзагроз та реалізації заходів реагування з боку держави. Науковець В.А. Ліпкан виділяє ключові кіберзагрози, які ставлять під загрозу національну безпеку України, серед яких:

– військова агресія з боку російської федерації, що включає використання кіберпростору як одного з інструментів впливу;

– недостатній рівень кіберграмотності та медіакультури населення, що ускладнює протидію дезінформації та кібератакам;

– відсутність комплексного підходу до комунікаційної політики на державному рівні, що негативно впливає на координацію у сфері кібербезпеки;

– вразливість критичної інфраструктури та офіційних електронних ресурсів України, особливо до атак хакерських угруповань;

– оральна застарілість та фізичний знос матеріальної бази кіберпростору, що обмежує можливості ефективної протидії загрозам;

– застарілість та недосконаліть існуючих методів боротьби з кіберзлочинністю, що не задовольняють необхідні потреби забезпечення кібербезпеки в межах протидії сучасним викликам;

– слабкість системи захисту державної таємниці, що створює ризики витоку критичної інформації.

Ці загрози демонструють нагальну потребу в модернізації інфраструктури, удосконаленні законодавчої бази та впровадженні ефективних механізмів реагування на кіберзагрози, які б відповідали сучасним викликам [15].

Механізми забезпечення інформаційної безпеки України можна умовно поділити на два ключові рівні: законодавчий та адміністративний.

Законодавчий рівень відіграє фундаментальну роль у формуванні нормативно-правової бази, що виступає регулятором відносини у сфері інформаційної безпеки, натомість якість забезпечення даного рівня визначає ефективність захисту інформаційного простору та запобігання можливим загрозам.

Адміністративний рівень охоплює діяльність спеціалізованих установ, завдання яких полягають у реалізації стратегічних цілей інформаційної безпеки. Основна мета заходів адміністративного рівня – це розробка й впровадження комплексної програми дій у сфері інформаційної безпеки, таких як виділення необхідних ресурсів, моніторинг їхнього використання та контроль виконання поставлених завдань.

Синергія між законодавчим і адміністративним рівнями є важливою умовою забезпечення ефективної роботи механізмів захисту інформаційної безпеки держави [9].

Головним стратегічним завданням інформаційної безпеки України є формування потужного національного інформаційного простору, що виступає ключовим елементом, який підтверджує присутність держави на глобальній інформаційній арені. Реалізація цього завдання передбачає створення ефективної системи протидії будь-яким інформаційним загрозам, захисту інформаційних ресурсів, інформаційного середовища та інфраструктурної бази країни. Даний підхід слугує фундаментом зміцнення позицій України в міжнародному інформаційному просторі та гарантування її національної безпеки [16].

Здійснення заходів з кіберзахисту передбачає кілька ключових етапів, кожен з яких спрямований на забезпечення надійності та безпеки національного кіберпростору. По-перше, ідентифікація включає виявлення реальних і потенційних кіберзагроз для запобігання та їх нейтралізації. На цьому етапі

важливо своєчасно визначити всі ризики, які можуть вплинути на інформаційні та технологічні системи.

По-друге, захист полягає в розробці та впровадженні методів, засобів і процедур кіберзахисту, що гарантують сталість функціонування інформаційних, телекомунікаційних та технологічних систем. Даний аспект включає забезпечення технічної та організаційної безпеки всіх критичних елементів інфраструктури [17].

Третім етапом є виявлення, яке включає проведення моніторингу та збору інформації про нетипові події в кіберпросторі для своєчасного реагування на потенційні загрози. Це дозволяє оперативно виявляти аномалії та визначати їхні джерела.

Реагування передбачає вжиття заходів для запобігання кіберінцидентам та мінімізації їхніх негативних наслідків, таких як загроза життю, здоров'ю людей або шкоди майну. Важливим аспектом є постійне удосконалення систем кіберзахисту з урахуванням актуальних та потенційних ризиків.

Нарешті, на етапі відновлення здійснюється поновлення штатного режиму функціонування інформаційно-телекомунікаційних та технологічних систем після наслідків кібератак. Це включає відновлення втрачених або пошкоджених даних, а також створення умов для розслідування наслідків атак [13].

У контексті кіберзахисту базисна інфраструктура повинна забезпечувати захист національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, а також об'єктів критичної інфраструктури. Важливими аспектами є також формування культури кібербезпеки на підприємствах різних форм власності та інформування громадян про наслідки кіберінцидентів, що сприятиме підвищенню обізнаності та готовності до кіберзагроз [13].

Отже, кіберзахист державних інформаційних ресурсів є основою національної безпеки, оскільки він гарантує стабільність та захищеність критично важливих інформаційних систем від кіберзагроз. Забезпечення ефективного кіберзахисту дозволяє зберегти конфіденційність, цілісність і доступність даних, що є необхідними для функціонування державних органів, економіки та інфраструктури.

1.3 Класифікація цифрових інструментів кіберзахисту державних інформаційних ресурсів

Кіберзлочинці постійно удосконалюють свої методи та технології, що вимагає застосування аналогічних засобів і програмного забезпечення для ефективної протидії. Швидке реагування на кіберінциденти є надзвичайно важливим, але без належного фінансування сучасних систем моніторингу та аналізу загроз ефективне виявлення та нейтралізація атак стають малоймовірними. Відсутність достатніх ресурсів для підтримки цих технологій значно знижує здатність системи оперативно реагувати на нові кіберзагрози, що матиме серйозні наслідки для подальшого забезпечення функціонування інформаційної безпеки [18].

Інтеграція штучного інтелекту (AI) та машинного навчання (ML) в сферу кібербезпеки є значним кроком уперед, оскільки ці технології дозволяють ефективно обробляти великі обсяги даних і здійснювати їх аналіз із високою швидкістю. Основною перевагою AI та ML є їхня здатність до самонавчання та гнучкої адаптації до нових типів кіберзагроз, що забезпечує швидкість реагування системи захисту інформаційних даних на актуальні зміни. З розвитком технологій загрози стають дедалі складнішими та різноманітнішими, що вимагає постійного удосконалення алгоритмів для виявлення і нейтралізації атак.

Крім того, ці інструменти здатні автоматизувати рутинні завдання, що забезпечує зростання ефективність роботи спеціалістів. Завдяки AI та ML можна не лише оперативно виявляти аномалії, але й прогнозувати потенційні загрози, що дає змогу запобігти атакам ще до їх початку. У майбутньому ці технології відіграватимуть все більш значущу роль у забезпеченні безпеки цифрових активів та захисту інформаційних систем. Водночас, розвиток даних технологій передбачає залучення значних інвестицій, навчання кваліфікованих кадрів і підтримку кіберінфраструктури [19]. Згідно з прогнозами звіту Cybersecurity Ventures, до 2025

року глобальні економічні збитки від кіберзлочинності можуть досягти 10,5 трильйонів доларів США [20].

Необхідність розвитку технічного забезпечення органів влади, відповідальних за кібербезпеку вказує на ще одну важливу проблему – дефіцит кваліфікованих спеціалістів у сфері кібербезпеки та обмежені можливості для підвищення їхньої кваліфікації, особливо серед тих, хто здобув освіту декілька років тому. Наявність даного аспекту значно ускладнює боротьбу з кіберзагрозами, і ця ситуація безпосередньо пов'язана з дефіцитом фінансування та ресурсів, оскільки недостатні інвестиції в розвиток людського капіталу стримують прогрес цієї галузі [7].

Кібератаки в останні роки набувають все більш складних і витончених форм, що вимагає від фахівців високого рівня кваліфікації та постійного оновлення їхніх знань. У світлі швидкого розвитку технологій у сфері кібербезпеки, професіонали повинні безперервно вдосконалювати свої навички, щоб ефективно протидіяти новим загрозам. Крім того, через високий попит на кваліфікованих спеціалістів у цій галузі на міжнародному ринку праці, Україна стикається з проблемами залучення та утримання таких кадрів. Тому особливу увагу варто приділяти створенню умов для розвитку професіоналів у країні, залученню інвестицій у цю сферу та заохоченню талановитих кадрів для довгострокової роботи в Україні.

Недостатня кількість кваліфікованих кадрів з кібербезпеки спричиняє затримки у виявленні та усуненні вразливостей, що в цілому зумовлює зниження ефективності реагування на кіберінциденти та підвищує ризики для інформаційної безпеки організацій. Це спричиняє збільшення кількості атак, оскільки організації не мають достатнього ресурсу для своєчасного реагування на загрози та запобігання їх розвитку. Брак кваліфікованих спеціалістів ускладнює швидке реагування на інциденти, що створює сприятливі умови для кіберзлочинців. Значна частина витоків даних виникає через людський фактор, коли співробітники допускають помилки через брак необхідних навичок. Крім того, недостатня кількість спеціалістів з цифрової криміналістики ускладнює розслідування

кіберзлочинів. Органи державної влади особливо відчувають дефіцит фахівців з кібербезпеки, що суттєво обмежує їхню здатність ефективно захищати інформаційні системи від потенційних загроз і кібернападів [13].

Нестача кваліфікованих фахівців у сфері кібербезпеки своєю чергою затримує процес розпізнавання та усунення вразливих точок, зменшує ефективність реагування на інциденти, водночас збільшуючи кількості кібератак. Через недостатню кількість професіоналів швидке й ефективне реагування на загрози стає складним, що створює сприятливі умови для кіберзлочинців. Багато випадків витоку даних спричинені людським фактором, зокрема помилками персоналу, який не має достатньої кваліфікації. Крім того, брак спеціалістів з цифрової криміналістики ускладнює розслідування кіберзлочинів. Державні органи особливо відчувають нестачу таких фахівців, що суттєво обмежує їхню здатність ефективно захищати інформаційні системи [18].

У сучасному цифровому середовищі, де технологічний прогрес призводить до безперервного зростання кіберзагроз, важливість кібербезпеки важко переоцінити. Від великих корпорацій до окремих користувачів, усі зіштовхуються з потребою захисту своїх цифрових активів. Це підкреслює необхідність використання ефективних цифрових інструментів для забезпечення кібербезпеки. Такі інструменти не лише сприяють виявленню та запобіганню кібератакам, а й захищають особисту інформацію та дані підприємств. Вони стають ключовим елементом будь-якої стратегії безпеки, яка пристосовується до постійно змінюваного кіберпростору.

Norton Antivirus – це потужний антивірусний програмний продукт, який забезпечує всебічний захист від вірусів, шпигунського програмного забезпечення та інших загроз. Він включає функції для охорони особистих даних і фінансових транзакцій під час роботи в інтернеті. Norton Antivirus пропонує багаторівневу безпеку, до якої входять брандмауер і система запобігання вторгненням. Крім того, програма гарантує автоматичні оновлення, що дозволяє користувачам завжди мати доступ до найновіших захисних можливостей [21].

Bitdefender славиться своїми інноваційними підходами в галузі кібербезпеки, пропонуючи надійний захист від усіх типів загроз. Цей програмний продукт забезпечує розширений захист від вірусів та онлайн-атак, а також засоби для охорони конфіденційності. Bitdefender містить функції контролю доступу до веб-камери та мікрофона, що додає додатковий рівень захисту приватності. Крім того, вона забезпечує багатошаровий захист від програм-вимагачів та шифрування даних для підвищення рівня безпеки [22].

McAfee – один з найвідоміших брендів у сфері кібербезпеки, який пропонує комплексні рішення для захисту різноманітних пристроїв. Цей програмний продукт забезпечує захист від вірусів, шпигунського ПЗ та інших загроз в інтернеті. McAfee також охороняє особисті дані та ідентичність користувачів, особливо під час онлайн-покупок і банківських транзакцій. Програма містить різноманітні інструменти для оптимізації роботи пристроїв та управління паролями [23].

Nessus, розроблений компанією Tenable Network Security, є одним із лідерів серед інструментів для сканування вразливостей. Цей продукт дозволяє виявляти та аналізувати вразливості в мережах і системах, підтримуючи широкий діапазон платформ. Nessus забезпечує детальний аналіз безпеки, включаючи перевірку на наявність відомих вразливостей, помилок конфігурації та можливостей для віддаленого доступу [24].

Wireshark є потужним інструментом для аналізу мережевого трафіку, що дає змогу користувачам перехоплювати та виводити детальні дані про мережеву активність. Цей аналізатор широко застосовується для діагностики мережевих проблем і дослідження мережевих протоколів, що сприяє виявленню підозрілих дій та уразливих місць у системі [25].

Snort, створений компанією Cisco Systems, є ефективною системою для виявлення та запобігання вторгненням, яка застосовується для моніторингу мережевої активності. Цей інструмент може працювати як у режимі виявлення, так і в режимі запобігання вторгненням, надаючи реальний захист від різних типів кібератак [26].

LastPass – це популярний інструмент для керування паролями, який дозволяє зберігати та організовувати паролі в захищеному цифровому сховищі. Цей менеджер паролів спрощує процес управління, генеруючи сильні та унікальні паролі для кожного облікового запису, а також автоматично заповнює поля для входу, що підвищує безпеку та зручність користування [23].

Nmap, також відомий як Network Mapper, є одним з найбільш поширених інструментів для сканування мереж. Він дозволяє виявляти активні пристрої в мережі, перевіряти відкриті порти та визначати використовувані протоколи і сервіси. Nmap є ключовим інструментом для мережевих адміністраторів, що допомагає забезпечувати безпеку та ефективне управління мережею [24].

Аналізуючи представлені цифрові інструменти кібербезпеки, стає зрозуміло, що кожен з них має свою специфіку та орієнтований на вирішення конкретних завдань захисту. Від антивірусних програм, які протистоять шкідливому ПЗ та вірусам, до систем керування паролями, що гарантують безпеку особистих даних – кожен інструмент має критичне значення для формування ефективної системи безпеки. Важливо обирати інструменти, що відповідають специфічним потребам і вимогам, а також регулярно оновлювати їх для підтримки належного рівня захисту. З огляду на стрімкий розвиток технологій і нових кіберзагроз, постійне навчання та підвищення обізнаності в галузі кібербезпеки є необхідністю як для окремих користувачів, так і для організацій [28].

Сучасні методи впровадження заходів кібербезпеки повинні базуватись на стратегічних документах та державних програмах, що передбачають модернізацію систем захисту, розвиток адміністративних і правових процедур, а також удосконалення технічних аспектів. Основними напрямами, які сприятимуть посиленню захисту як держави, так і корпоративного сектору, є оновлення нормативно-правових актів для імплементації міжнародних стандартів кіберзахисту та боротьби з кіберзлочинністю, впровадження інновацій у засобах захисту цифрової інфраструктури, залучення міжнародного досвіду та застосування надійних програмних рішень для забезпечення належного рівня безпеки.

Забезпечення стійкості держави до кіберзагроз є критично важливим завданням, особливо в умовах триваючої російської агресії. Це вимагає посиленої уваги до захисту національних інформаційних ресурсів та розробки стратегій для збереження їх цілісності та доступності в умовах зростаючих кіберзагроз. Можна виділити кілька стратегій для зміцнення кіберстійкості держави (рис.1.4).

З урахуванням Національної стратегії кібербезпеки Великобританії наразі впроваджується новий формат співпраці між державою та приватним сектором у сфері кібербезпеки – Партнерство з обміну інформацією з кібербезпеки (Cybersecurity Information Sharing Partnership, CISP). Метою CISP є створення безпечної платформи для обміну інформацією між урядом та бізнесом, що сприятиме посиленню інформаційної безпеки. Згідно із законодавством, британські оператори даних зобов'язані запроваджувати необхідні технічні й організаційні заходи для захисту від несанкціонованої обробки даних. За серйозні порушення кібербезпеки можуть бути накладені штрафи до £500,000. Крім того, фінансові установи повинні дотримуватися спеціальних вимог, зокрема щодо контролю за дотриманням фінансових норм [11].

Рисунок 1.4 – Стратегії зміцнення кіберстійкості держави

Джерело: [1]

Отже, цифрові інструменти кіберзахисту державних інформаційних ресурсів відрізняються за функціональним призначенням і способами забезпечення безпеки, що дозволяє ефективно реагувати на сучасні кіберзагрози. Антивірусні програми, такі як Norton, Bitdefender та McAfee, забезпечують захист від шкідливого програмного забезпечення, вірусів і шпигунських програм, сприяючи захисту персональних і фінансових даних. Інструменти для аналізу мережевого трафіку, такі як Wireshark, дозволяють перехоплювати й досліджувати дані, що допомагає виявляти аномалії та потенційні загрози. Системи виявлення і запобігання вторгненням, зокрема Snort, контролюють мережеву активність, забезпечуючи захист у режимах моніторингу й активного запобігання. Інструменти для сканування вразливостей, як-от Nessus і Nmap, дозволяють ідентифікувати слабкі місця в мережевих інфраструктурах і конфігураціях, що є важливим етапом профілактики атак. У сукупності, класифікація цифрових інструментів кіберзахисту забезпечує комплексний підхід до захисту державних інформаційних систем, підвищуючи стійкість до кібератак та підтримуючи безпеку даних.

Висновок до розділу 1.

Державна система кіберзахисту відіграє основну роль у забезпеченні національної безпеки та ефективної роботи державних органів. Водночас забезпечення ефективного захисту в інформаційному просторі сприяє не лише стабільній роботі державних інституцій, а й виступає рушійним механізмом модернізації системи державного управління в цілому.

Вдосконалення моделей збереження конфіденційності й цілісності даних у векторі автоматизації та адаптації нормативно-правового забезпечення залишається одним з пріоритетних напрямів розвитку цифрових платформ та електронних послуг, що своєю чергою виступає суттєвим фундаментом для розвитку сучасної цифрової економіки.

Важливими елементами системи захисту даних виступають інструменти кіберзахисту, варіативність яких забезпечує можливість ефективно попереджати та протидіяти загрозам в інформаційному просторі.

РОЗДІЛ 2
ПРАКТИКА КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В УКРАЇНІ

2.1. Нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів

Правова основа кіберзахисту державних інформаційних ресурсів України включає низку ключових нормативно-правових актів, серед яких Конституція України та закони, що регулюють національну безпеку, внутрішню і зовнішню політику, а також електронні комунікації. Зокрема, це закони, що визначають правила захисту інформаційних ресурсів держави та інформації, яка підлягає правовій охороні. Крім того, важливими елементами правового забезпечення є міжнародні угоди, включаючи Конвенцію про кіберзлочинність, що були ратифіковані Верховною Радою України, а також укази Президента, постанови Кабінету Міністрів України та інші акти, спрямовані на виконання національних законів і міжнародних зобов'язань у сфері кібербезпеки. Це дозволяє створити єдину правову структуру для забезпечення стійкості державних інформаційних систем до кіберзагроз.

Правове регулювання кіберзахисту державних інформаційних ресурсів здійснюється як на міжнародному, так і на національному рівнях. Ключовим міжнародним документом у галузі кіберзахисту, ратифікованим Верховною Радою України, є Конвенція про кіберзлочинність [13]. У цьому документі наголошується на важливості запобігання діям, які порушують конфіденційність, цілісність і доступність комп’ютерних систем, мереж і даних, а також на боротьбі з їх неналежним використанням. В рамках Конвенції визначено кримінальну відповідальність за вказані правопорушення, надано повноваження для ефективного розслідування та переслідування таких злочинів, а також окреслено

механізми для їх виявлення та попередження. Особлива увага приділяється організації взаємодії як на національному рівні, так і в рамках міжнародного співробітництва, забезпечуючи швидкі та надійні механізми координації зусиль [13].

Нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів на національному рівні забезпечується через наступні закони (рис.2.1).

Рисунок 2.1 – Закони України, які регулюють кіберзахист державних інформаційних ресурсів на національному рівні

Джерело:[31;32;33;34;35;36;37;38;39;40;41;2;4;71;30]

Певні закони безпосередньо формулюють правові основи для регулювання кіберзахисту державних інформаційних ресурсів, чітко визначаючи механізми та процедури цього процесу. Водночас інші закони торкаються питання кіберзахисту лише в окремих аспектах, відводячи йому лише частину регулюючих норм, які можуть бути застосовані у контексті більш широких правових принципів та загальних засад [29].

Відповідно до статті 17 Конституції України, захист інформаційної безпеки є однією з ключових функцій держави та спільною справою всього українського народу. Вектор зовнішньополітичної діяльності у сфері інформаційної безпеки регулює Стаття 18 Конституції України, яка підкреслює спрямованість держави на забезпечення національних інтересів та безпеки через підтримку мирного та взаємовигідного співробітництва з іншими державами на основі міжнародних норм і принципів. Водночас стаття 106 Конституції надає Президенту України ключову роль у забезпеченні національної безпеки, що включає в себе і кібербезпеку, гарантування захисту національних інтересів у цифровому просторі [30].

Основним нормативно-правовим актом, що регулює кіберзахист державних інформаційних ресурсів на національному рівні, є Закон України «Про основні засади забезпечення кібербезпеки України». Даний закон вказує на організаційно-правові та технічні основи для забезпечення безпеки інформаційних ресурсів, визначаючи механізми захисту від кіберзагроз, а також органи, відповідальні за їх реалізацію та координацію національної політики в сфері кібербезпеки [31].

Вперше в рамках Закону про кібербезпеку були представлені чіткі визначення ряду термінів, зокрема «кібербезпека», «кіберзагроза», «кіберпростір», «кіберінцидент», «кібершпіонаж» та «кібертероризм». Раніше в українському законодавстві уникали використання терміну «кібер», застосовуючи терміни «інформація» або «електронний» для регулювання питань, що стосуються кібербезпеки. Хоча в Стратегії кібербезпеки використано низку термінів, що містять префікс «кібер», самі визначення цих термінів у документі відсутні. Таким чином, нові терміни, що вводяться в Законі про кібербезпеку, не завжди співвідносяться з тими, що застосовувалися раніше в інших нормативних актах.

Враховуючи це, важливо здійснити всебічний аналіз законодавства на предмет його узгодження з положеннями новоприйнятого Закону [31].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», відповідальність за забезпечення кібербезпеки покладається на широкий спектр органів та організацій. До них належать не лише міністерства та центральні органи виконавчої влади, але й органи місцевого самоврядування, місцеві державні адміністрації, а також правоохоронні, розвідувальні та контррозвідувальні служби. У сферу кібербезпеки також залучаються Збройні Сили України та інші військові формування, які діють відповідно до законодавства, до яких належить оперативно-розшукова діяльність. Важливу роль у захисті інформаційних ресурсів також відіграють Національний банк України та підприємства, установи й організації, що складають частину критичної інфраструктури країни, оскільки їхня безпека безпосередньо впливає на стабільність держави. Перелічені органи і установи здійснюють ряд функцій, а саме: виявлення, попередження та розслідування кіберзлочинів, захист критичних об'єктів і інформаційних ресурсів держави, розробку та впровадження стратегій і заходів кіберзахисту, а також участь у міжнародному співробітництві в сфері кібербезпеки та підвищення кіберсвідомості серед громадян і бізнесу [31].

Закон України «Про оборону України» визначає роль кібербезпеки як складову національної оборони, забезпечуючи захист державних інформаційних ресурсів від кіберзагроз, що можуть виникнути під час військових конфліктів [32]. Закон України «Про національну безпеку України» закріплює основи кібербезпеки як стратегічного елемента національної безпеки, та як такого, що сприяє інтеграції кіберзахисту державних інформаційних ресурсів в загальну систему безпеки країни [33]. Закон України «Про ратифікацію Конвенції про кіберзлочинність» регулює правові основи для міжнародного співробітництва в боротьбі з кіберзлочинністю, що забезпечує захист українських державних інформаційних ресурсів від глобальних кіберзагроз [34]. Закон України «Про інформацію» визначає основні принципи регулювання інформаційних відносин, включаючи захист інформаційних ресурсів держави [35]. Закон України «Про державну таємницю»

встановлює вимоги щодо захисту інформації, що має статус державної таємниці, у тому числі в кіберпросторі, з метою запобігання витоку важливих державних даних [36]. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» визначає повноваження органів, відповідальних за забезпечення кібербезпеки, у тому числі захист державних інформаційних ресурсів від кіберзагроз [37]. Закон «Про захист інформації в інформаційно-телекомунікаційних системах» регулює заходи захисту інформації, що зберігається та передається через інформаційно-телекомунікаційні системи, впливаючи на кіберзахист державних інформаційних ресурсів [38]. Закон «Про електронні документи та електронний документообіг» визначає правила використання електронних документів та їх захисту, що важливо для забезпечення кібербезпеки в державних інформаційних системах [39]. Закон України «Про національну поліцію» надає поліції повноваження для розслідування кіберзлочинів, що впливає на забезпечення кіберзахисту державних інформаційних ресурсів [40]. Закон України «Про Службу безпеки України» надає СБУ повноваження для виявлення та попередження кіберзагроз, що сприяє захисту критично важливих державних інформаційних ресурсів [41]. Закон України «Про Національну програму інформатизації» визначає стратегічні напрямки розвитку інформаційних технологій в Україні, включаючи забезпечення кіберзахисту державних інформаційних ресурсів як частину загальної інформатизації [2]. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» забезпечує узгодження норм законодавства щодо доступу до інформації та її захисту, сприяючи створенню правової основи для кіберзахисту публічної інформації [4].

Закон України «Про Раду національної безпеки і оборони України» регулює діяльність цього органу, визначаючи його роль у забезпеченні національної безпеки та оборони країни, включаючи координацію заходів щодо кіберзахисту державних інформаційних ресурсів. Рада національної безпеки і оборони України здійснює розробку та розгляд питань, що стосуються захисту національних

інтересів, таких як напрямки забезпечення кібербезпеки як складову національної безпеки України. Вона також здійснює низку заходів у сфері інформаційної безпеки, спрямованих на захист інформаційної інфраструктури, зокрема заходи для протидії цифровим атакам у кіберпросторі. Рада проводить стратегічну оцінку поточного стану та перспектив розвитку кібербезпеки, ґрунтуючись на інформації від суб'єктів кібербезпеки щодо загального стану кібербезпеки в державі. Це підкреслює важливість координаційної ролі Ради в забезпеченні кібербезпеки [6].

Наступною категорією нормативно-правових актів, що регулюють питання забезпечення інформаційної безпеки є постанови Кабінету Міністрів України. Ці акти встановлюють конкретні механізми реалізації державної політики в області захисту інформаційних ресурсів, визначають обов'язки державних органів, підприємств та організацій щодо виконання заходів з інформаційної безпеки, а також сприяють розвитку правової інфраструктури для ефективного реагування на сучасні кіберзагрози (рис. 2.2).

Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» окреслює основні вимоги щодо належного рівня захисту для ключових державних ресурсів від кіберзагроз [42]. Постанова КМУ «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» регулює процес регулярного оцінювання стану кіберзахисту важливих державних інформаційних об’єктів, що дозволяє своєчасно виявляти уразливості та здійснювати коригування заходів [43]. Постанова КМУ «Деякі питання об’єктів критичної інформаційної інфраструктури» визначає порядок класифікації об’єктів критичної інформаційної інфраструктури. Дана постанова слугує важливим елементом координації їх кіберзахисту, а також регулює впровадження відповідних заходів з підтримки їх захисту від загроз [44].

Рисунок 2.2 – Постанови КМУ, які регулюють кіберзахист державних інформаційних ресурсів на національному рівні

Джерело:[42;43;44;45;46;47;48;49;50]

Постанова КМУ «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» визначає заходи щодо підтримки функціонування критично важливих інформаційно-комунікаційних систем в умовах воєнного стану, забезпечуючи неперервність їх роботи та кіберзахист [45]. Постанова КМУ «Деякі питання подання інформації у сфері захисту критичної інфраструктури» регламентує правила поширення інформації

про стан захисту критичної інфраструктури для належного моніторингу та взаємодії органів влади [46]. Постанова КМУ «Про затвердження Регламенту обміну інформацією між суб'єктами національних систем захисту критичної інфраструктури» встановлює процедури обміну інформацією між суб’єктами, відповідальними за захист критичної інфраструктури, тим самим дозволяє покращити координацію та оперативність у реагуванні на кіберзагрози [88]. Постанова КМУ «Деякі питання паспортизації об'єктів критичної інфраструктури» регламентує процес сертифікації об’єктів критичної інфраструктури з метою належного обліку об’єктів критичної інфраструктури та забезпечення необхідного рівня захисту [47]. Постанова КМУ «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» встановлено порядок ведення Реєстру критичної інфраструктури. Це дозволяє своєчасно реагувати на загрози та вживати заходів щодо їх захисту [48]. Постанова КМУ «Про затвердження Положення про організаційно-технічну модель кіберзахисту» визначає основи організаційно-технічної моделі кіберзахисту для державних інформаційних ресурсів, що включає інструменти та методи для їх ефективного захисту від кіберзагроз [49]. Постанова КМУ «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» регламентує проведення незалежних аудитів для оцінки ефективності систем кіберзахисту на об’єктах критичної інфраструктури, завдяки чому можна визначити рівень їхньої безпеки та вжити необхідних заходів для удосконалення захисту [50].

Систему законодавчого забезпечення захисту національних інформаційних ресурсів становлять не лише основні закони, але й низка підзаконних актів, особливого значення у яких відіграють укази Президента України. Дані нормативні стратегії визначають основні напрями, що регулюють державну політику в сфері кібербезпеки. Зокрема, вони охоплюють такі документи, як Стратегія національної безпеки України, Концепція розвитку сектору безпеки і оборони України, Стратегія кібербезпеки України, Стратегія воєнної безпеки України, Стратегія інформаційної безпеки та інші нормативні акти. Ці стратегії не тільки окреслюють пріоритети

щодо удосконалення кіберзахисту, але й формують правову основу для координації дій між різними державними органами, що необхідно для своєчасного і ефективного реагування на кіберзагрози та виклики національної безпеки.

Для забезпечення захисту інформації та національних інформаційних ресурсів прийнято постанову Кабінету Міністрів України «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» [50]. Відповідно до цього рішення міністерства, органи виконавчої влади, а також державні підприємства, підприємства місцевого самоврядування, установи та підпорядковані їм організації мають право призупиняти або обмежувати роботу інформації, інформаційних комунікацій та електронної інформації в умовах воєнного стану. Дані заходи спрямовані на забезпечення безперебійного функціонування таких систем і захисту оброблюваної в них інформації, зокрема, державних інформаційних ресурсів. Обмеження діють до моменту припинення або скасування воєнного стану. Перелік відкритих даних у сфері охорони довкілля, доступ до яких може бути обмежено, визначено в додатку А [3].

Отже, Україні вдалося досягти значних результатів у сфері нормативно-правового регулювання інформаційної безпеки. Наявні особливості функціонування системи обумовлено тим, що забезпечення інформаційної безпеки стало одним із основних пріоритетів органів публічної адміністрації.

Сучасне інформаційне середовище має великий вплив на політичну, економічну, військову та інші сфери національної безпеки України.

Аналіз чинних нормативно-правових актів показує, що інформаційна безпека є невід'ємною частиною національної безпеки, що вимагає розробки ефективних механізмів захисту інформаційних ресурсів, систем їх формування, обробки та поширення, а також захисту інформаційної інфраструктури, конфіденційної, службової та персональної інформації.

2.2. Система національної безпеки в кіберекономічному просторі

Національна безпека – це категорія, яка визначає рівень захищеності основних інтересів, прав і свобод громадян та держави від внутрішніх і зовнішніх загроз. Вона також відображає відсутність загроз для прав і свобод людини, а також для базових інтересів та цінностей, важливих для суспільства та держави. Національна безпека є складною і багатовимірною системою, що включає різні підсистеми та елементи. Основними компонентами національної безпеки є політична, економічна, воєнна, соціальна, екологічна, інноваційна та науково-технологічна безпека, які взаємодіють і взаємозалежні між собою. Кожен із цих аспектів має важливе значення для забезпечення стабільності та розвитку держави в умовах зовнішніх і внутрішніх загроз [13].

Основні принципи державної політики, що орієнтована на захист національних інтересів та забезпечення безпеки громадян, суспільства і держави від внутрішніх і зовнішніх загроз, визначені в Законі України «Про національну безпеку України». Цей закон формулює ключові напрямки національної безпеки, забезпечуючи комплексний підхід до захисту державних інтересів та встановлює правові засади для ефективної діяльності органів державної влади в умовах потенційних загроз різного характеру. У цьому законі надані визначення ключових термінів (рис.2.3).

Державна політика в галузі національної безпеки та оборони спрямована на захист від різноманітних загроз, насамперед у сферах військової, зовнішньополітичної, національної, економічної, інформаційної та екологічної безпеки. Особлива увага приділяється безпеці критичної інфраструктури, кібербезпеці та інших ключових складових, що забезпечують стабільність і функціонування держави в умовах як внутрішніх, так і зовнішніх викликів. Ця політика передбачає скоординовані дії органів влади, спрямовані на створення стійкої системи захисту від можливих загроз на всіх рівнях державного управління [33].

Рисунок 2.3 – Ключові терміни системи національної безпеки

Джерело: [33]

Рівень розвитку та безпека інформаційного та кіберпростору є одними з ключових факторів, що суттєво впливають на політичну, економічну та інші сфери національної безпеки України. Тому, інформаційну безпеку та кібербезпеку доцільно розглядати як складові частини інших аспектів національної безпеки. Проте, водночас вони є самостійними компонентами, що мають подвійний характер. Це зумовлено кількома важливими факторами (рис.2.4).

Інформаційні та кіберстратегії набувають особливої важливості в контексті реалізації політичних стратегій співдружності, виступаючи своєрідною «зброєю» в умовах стратегії суперництва. Вони є необхідними інструментами для досягнення національних цілей у глобальному конкурентному середовищі.

Інформаційна безпека та кібербезпека є ключовими складовими національної безпеки України, що визначені окремо у Законі України «Про національну безпеку України». Їх належне забезпечення, за умови ефективної національної інформаційної політики, має значний вплив на успішне виконання завдань у політичній, воєнно-політичній, воєнній, економічній, соціальній та інших сферах державної діяльності. Зокрема, ефективна інформаційна політика здатна

сприяти зниженню геополітичної напруженості та забезпеченню миру через вирішення зовнішньополітичних і воєнних конфліктів [16].

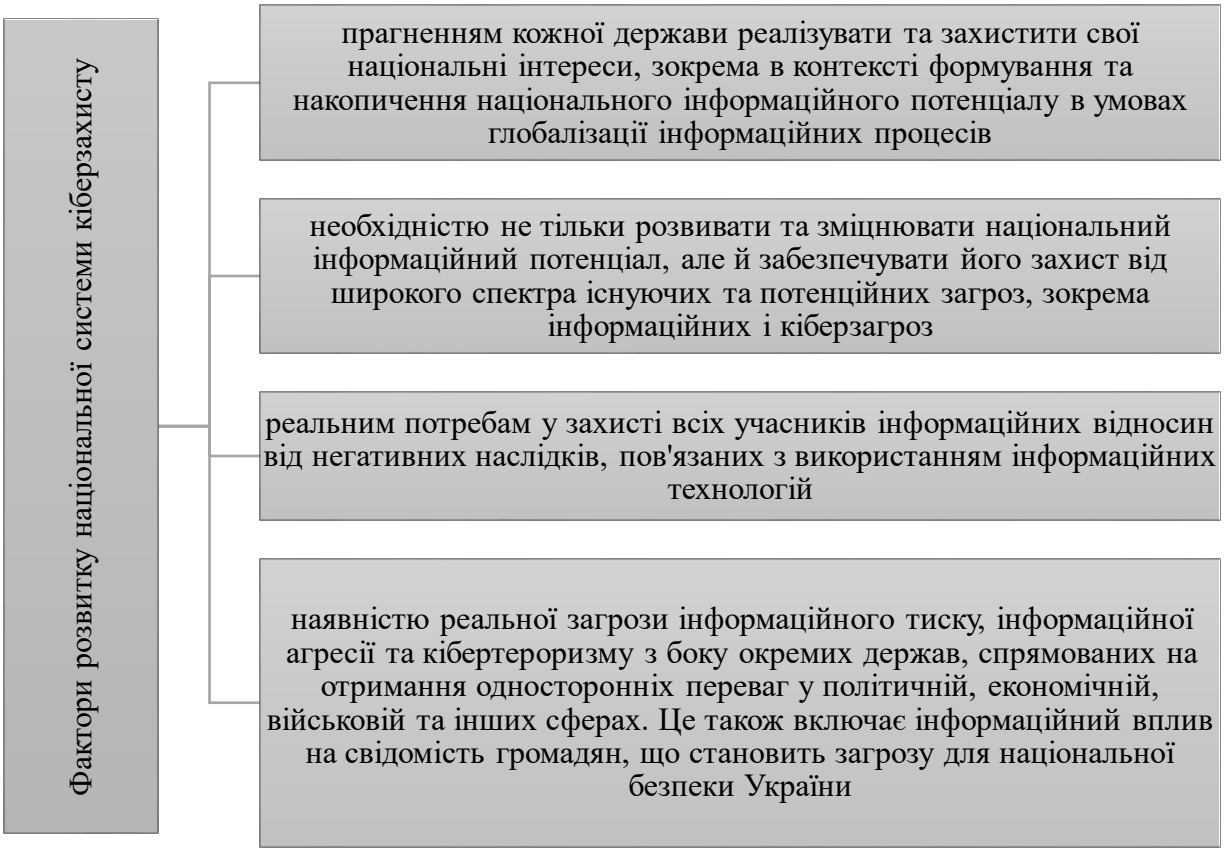

Рисунок 2.4 – Фактори розвитку національної системи кіберзахисту

Джерело: [33]

За роки незалежності України було сформовано основні складові системи забезпечення інформаційної безпеки та кібербезпеки. Зокрема, створено нормативно-правову базу для регулювання цих сфер, визначено функції та повноваження державних органів, які відповідають за інформаційну безпеку.

Національна система забезпечення інформаційної безпеки – це організоване поєднання державних органів, збройних сил і засобів захисту інформації, що функціонує на основі закону та під судовим контролем. Дана система виступає важливою ланкою в загальній архітектурі інформаційної безпеки, яка охоплює як особистість, суспільство, так і націю в цілому та забезпечує їх правовий захист [51].

Стратегія кібербезпеки передбачає створення національної системи кібербезпеки, спрямованої на забезпечення безпечного функціонування та використання кіберпростору в інтересах людини, суспільства та нації.

Система протидії кібернетичним загрозам є сукупністю узгоджених елементів, кожен з яких виконує конкретні завдання в межах єдиного плану і стратегії. Ці елементи формуються та розгортаються в кіберпросторі задля забезпечення безпеки та належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [28].

Органи управління інформаційною безпекою можна класифікувати на загальні, контрольні та спеціалізовані. До загальних органів управління належать ті, що функціонують на національному рівні. На найвищому щаблі в ієрархії органів, відповідальних за інформаційну безпеку, перебувають Верховна Рада України, Президент України та Рада Національної безпеки і оборони України (РНБО). Верховна Рада через свої профільні комітети відповідає за розробку законодавства, яке регулює сферу інформаційної безпеки, в той час як Президент та РНБО координують діяльність усіх суб'єктів цієї сфери, визначаючи стратегічні напрямки і пріоритети національної безпеки [51].

Кабінет Міністрів України, через свої структурні підрозділи, зокрема Управління стратегії розвитку інформаційних технологій, реалізує державну політику в галузі інформаційної безпеки. Даний орган забезпечує координацію між різними державними органами та організаціями, сприяючи ефективному впровадженню заходів, які гарантують захист інформаційної інфраструктури країни та відповідних технологій.

Регуляторні та контрольні органи відіграють ключову роль у забезпеченні стабільності та безпеки інформаційного простору країни. Одним з основних органів, що здійснює контроль за медіапростором, є Національна Рада України з питань телебачення та радіомовлення, яка відповідає за моніторинг дотримання законодавчих норм у засобах масової інформації, забезпечуючи їх збалансованість, незалежність і відповідність стандартам, що регулюють інформаційну діяльність.

Цей орган також сприяє розвитку вільного та демократичного медіапростору, що відповідає вимогам сучасного інформаційного середовища [11].

Генеральна прокуратура України і судова система виконують важливі функції з правового захисту в сфері інформаційної безпеки, займаючись розглядом справ, пов’язаних з порушеннями в цій галузі. Зокрема, прокуратура виступає у ролі наглядача за дотриманням законів, а суди забезпечують правосуддя в питаннях, що стосуються порушень прав на інформацію, кіберзлочинності, а також порушень прав громадян і державних органів.

Спеціалізовані органи займаються більш вузькими напрямками забезпечення інформаційної безпеки. Одним з найбільш важливих суб'єктів у цій сфері є Служба безпеки України (СБУ), яка відіграє вирішальну роль у захисті державних інформаційних ресурсів від зовнішніх і внутрішніх загроз. СБУ відповідає за забезпечення криптографічного захисту державної інформації, протидію кіберзлочинності, а також захист критичної інфраструктури від кібератак і інших кіберзагроз [51].

Згідно з п. 3 ч. 2 ст. 3 Закону України «Про основні засади забезпечення кібербезпеки України» [31], СБУ здійснює заходи для запобігання, виявлення, припинення і розслідування злочинів, вчинених у кіберпросторі, які загрожують безпеці людства. СБУ активно проводить контррозвідувальні і оперативно-розшукові дії, спрямовані на боротьбу з кібертероризмом і кібершпигунством, здійснює перевірку готовності об'єктів критичної інфраструктури до можливих кібератак і інцидентів, а також розслідує кіберінциденти, що можуть вплинути на безпеку державних електронних ресурсів. Важливим аспектом є також реагування на кіберінциденти в межах державної безпеки, що передбачено в Стратегії інформаційної безпеки 2022 року. Повноваження СБУ в контексті інформаційної безпеки визначені Законом «Про Службу безпеки України», що регламентує її діяльність у сфері захисту державних інтересів у кіберпросторі та боротьбі з кіберзагрозами [41].

Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку) є одним з найважливіших органів, що забезпечує інформаційну

безпеку країни. Згідно з Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» (2006), ця служба здійснює важливі функції, спрямовані на забезпечення стабільності та безпеки державних інформаційних ресурсів.

Основні компетенції Держспецзв'язку включають:

1. Забезпечення урядового зв'язку. Держспецзв'язку займається розробкою та підтримкою державних систем урядового та конфіденційного зв'язку, що забезпечують безперебійне та безпечне спілкування між вищими органами державної влади. Це сприяє ефективному управлінню та координації в критичних ситуаціях.

2. Реалізація державної політики у сфері забезпечення захисту інформації. Організація відповідає за розробку, впровадження та контроль за виконанням заходів, спрямованих на технічний захист інформації. Даний вектор включає в себе як захист від несанкціонованого доступу, так і запобігання витоку або маніпуляціям з державними даними.

3. Комплексний захист інформаційних ресурсів. Держспецзв'язку забезпечує комплексний захист інформаційно-телекомунікаційних систем, включаючи запобігання несанкціонованому доступу, втручанню та знищенню інформаційних ресурсів. Це особливо важливо для захисту критичних інфраструктур, що мають стратегічне значення для функціонування держави.

4. Контроль та нагляд. Держспецзв'язку виконує функції моніторингу стану безпеки спеціальних видів зв'язку, а також контролює відповідність заходів захисту інформації встановленим національним стандартам і нормам. Це забезпечує систематичний контроль за рівнем інформаційної безпеки в державних структурах.

Для реагування на інциденти у сфері інформаційної безпеки створено команду реагування на надзвичайні ситуації в області комп'ютерних ситуацій України (CERT-UA) як структурний підрозділ Національного центру кіберзахисту, що діє у складі Держспецзв'язку та захисту інформації.

Отже, Держспецзв’язку є ключовим органом, що займається захистом інформаційного простору України на всіх рівнях – від криптографічного захисту до технічних заходів протидії кіберзагрозам. Її діяльність є невід’ємною частиною стратегії національної безпеки, яка має вирішальне значення для захисту держави від сучасних інформаційних викликів та загроз [37].

Ефективність роботи суб’єктів системи забезпечення інформаційної безпеки України вимагає дотримання їх постійної взаємодії. Дана властивість пов'язана з тим, що кожен елемент кібербезпеки спеціалізується на виконанні конкретних завдань відповідно до своїх повноважень і компетенції. Важливим аспектом є використання визначених законодавством адміністративно-правових форм та методів у межах своїх функцій. Така взаємодія дозволяє цим суб’єктам ефективно доповнювати один одного, що сприяє створенню єдиної, узгодженої організаційно-функціональної системи. Вона об’єднує суб’єктів не тільки через систему владно-розпорядчих повноважень, а й через спільну мету – забезпечення інформаційної безпеки [16]. Об'єктами цієї системи є:

– інтереси органів виконавчої влади в інформаційній сфері, що охоплюють питання безпеки інформації, що стосується функціонування державних органів;

– безпосередньо органи виконавчої влади, їх компетентні особи та взаємодія між ними, що включає суспільні відносини в інформаційній сфері, які формують основу для регулювання інформаційної безпеки;

– система забезпечення інформаційної безпеки України, яка складається з комплексних заходів і інститутів, що визначають політику і механізми захисту інформації на рівні держави [10].

Наведені елементи утворюють цілісну структуру, яка має на меті максимальне забезпечення стабільності та безпеки інформаційного середовища країни.

Основні завдання системи забезпечення інформаційної безпеки України включають:

– виявлення та прогнозування загроз, які можуть завдати шкоди життєво важливим інтересам особи, суспільства, нації;

– здійснення комплексу заходів як оперативного, так і довготривалого характеру для попередження і усунення таких загроз;

– формування та підтримання готовності сил і засобів, що забезпечують інформаційну безпеку, до ефективного реагування на будь-які загрози [17].

Для ефективної реалізації цих завдань потрібна чітко організована система органів, здатна виконати функції захисту інформаційного простору, складовими якої виступають чотири взаємопов'язані рівні:

1. Управлінські та адміністративні функції, що зосереджуються в межах управління Кабінету Міністрів України, який забезпечує координацію і стратегічне управління в галузі інформаційної безпеки.

2. Правоохоронні функції та забезпечення національної безпеки, що здійснюються органами, підпорядкованими Президенту України, і включають в себе боротьбу з кіберзлочинністю та іншими загрозами інформаційній безпеці.

3. Законодавче забезпечення та парламентський контроль, які виконуються Верховною Радою України, що полягає у розробленні законодавства, контролю за дотриманням стандартів у сфері інформаційної безпеки.

4. Приватна ініціатива, комерційні інтереси та громадський контроль, що здійснюється через діяльність неурядових організацій, незалежних ЗМІ та інших організацій, які сприяють розвитку та підтримці інформаційної безпеки на національному рівні [51].

Такий багаторівневий підхід дозволяє створити ефективну і комплексну систему забезпечення інформаційної безпеки України, де кожен рівень відповідає за виконання конкретних завдань та функцій.

Для перших трьох рівнів система забезпечення національної безпеки носить обов'язковий характер, що контролюється та забезпечується державними органами, в той час як для четвертого рівня – це радше моральний імператив. Діяльність недержавного сектору є важливою складовою забезпечення двостороннього зв'язку та взаємодії між громадськістю і державними органами. Однак цей сектор має свої вразливості, адже саме недержавні організації можуть стати привабливими цілями для розвідувальної діяльності іноземних спецслужб, а

також виступати ефективними інструментами для реалізації зовнішнього інформаційного впливу [11].

З одного боку, національні інтереси підтримуються такими цінностями, як патріотизм і злагоджена робота системи забезпечення інформаційної безпеки. З іншого боку, існують матеріальні стимули, як гранти, контракти та фонди, які можуть сприяти невиправданому залученню недержавних організацій до діяльності, що не завжди відповідає інтересам вітчизняної системи безпеки. Таким чином, питання легальності їх діяльності та залежність від іноземних замовників є важливими чинниками, що можуть впливати на ефективність і національну безпеку в цілому [5].

Одним із головних завдань системи інформаційної безпеки України є захист національних інтересів в інформаційному просторі. Серед основних функцій цієї системи перелічені у дод.Б. Загалом функції систем захисту інформації є взаємопов’язаними та комплексними та сприяють зміцненню національної безпеки в контексті сучасних викликів інформаційного середовища [11].

Україна розвиває комплексну та багаторівневу систему управління інформаційною безпекою, яка ефективно відповідає на сучасні виклики, такі як кібератаки, інформаційні війни, шпигунство та зовнішнє втручання у внутрішні справи держави. У цій системі основну роль виконує Державна служба спеціального зв'язку та захисту інформації, яка координує заходи, спрямовані на забезпечення криптографічного та технічного захисту інформаційних ресурсів. Її діяльність забезпечує не лише стабільність і надійність зв'язку між державними органами, але й інтегрований захист інформаційних систем, що гарантує інформаційну безпеку на всіх рівнях державного управління та прийняття рішень.

2.3. Стан розвитку кібербезпеки України

Забезпечення інформаційної безпеки є однією з основних проблем для кожної країни, особливо в умовах швидкого розвитку цифрових технологій та зростаючих кіберзагроз. В Україні це питання набуло особливого значення через численні внутрішні та зовнішні загрози.

Згідно зі Стратегією інформаційної безпеки, до основних національних викликів та загроз в Україні можна віднести (рис.2.5).

Рисунок 2.5 – Основні виклики та загрози національній системі кіберзахисту України

Джерело: [63]

Україна стикається з істотним тиском з боку кіберзлочинності, що проявляється у високій активності хакерських груп. В умовах російсько-

української війни кількість кібератак на державні та комерційні об'єкти значно зросла.

За даними Microsoft, ще до початку широкомасштабного вторгнення в 2022 році Україна була однією з найбільш уразливих країн у світі для кібератак, поступаючись лише США. У 2022 році, після початку війни, кількість кіберінцидентів різко збільшилася, а урядова команда CERT-UA зафіксувала понад дві тисячі атак. Це свідчить про надзвичайно високий рівень кіберзагроз, з якими зіштовхується країна в умовах війни [52].

З кінця березня 2022 року кібератаки на Україну набули масштабного характеру, включаючи фішингові атаки на електронні адреси урядових установ та збройних сил, що сталися 17 та 18 березня. Водночас, використання бекдора LoadEdge дозволило зловмисникам встановити шпигунське програмне забезпечення на комп'ютерах, починаючи з 20 березня. Напади на вебсайти Укртелекому та платформу WordPress 28 березня спричинили збої в комунікаціях та обмежили доступ до ключових фінансових і урядових ресурсів.

30 березня 2022 року було застосовано інформаційний викрадач MarsStealer, що дозволив отримати доступ до особистих даних громадян і організацій України. У квітні хакери також захопили банківські та платіжні дані через троянські програми 14 числа та фальшиві опитування в соціальних мережах, що відбулися 19 квітня 2022 року [53].

Українські владні органи зафіксували понад 85 хакерських груп, які мають негативний вплив на кібербезпеку країни, більшість з яких пов'язані з Росією, що є агресором у війні проти України. Однак, попри ці загрози, Україна активно розвиває свої кіберзахисні можливості. Згідно з Національним індексом кібербезпеки, Україна займає 24-те місце серед 160 країн, що є досить високим показником і свідчить про ефективність вжитих заходів у сфері кіберзахисту. Проте вітчизняна система не позбавлена слабких місць, що вимагає подальшого вдосконалення для підвищення ефективності кіберзахисту у майбутньому [53].

Кібератаки представляють серйозну загрозу для різних галузей економіки, включаючи енергетику, промисловість, логістику, телекомунікації та програмне

забезпечення. Однак найбільш небезпечні та руйнівні напади останнім часом орієнтовані на фінансовий сектор України, зокрема великі банки. Такі атаки серйозно впливають на національну економічну стабільність, особливо на довіру до фінансових установ та на безпеку фінансових операцій, що, у свою чергу, створює ризики для економічного зростання та національної безпеки.

Згідно з офіційним звітом Держспецзв'язку України за 2023 рік, кількість кібератак зросла на 15,9% порівняно з 2022 роком, досягнувши 2543 інцидентів. У другій половині 2023 року було зафіксовано та розслідувано 1460 кіберінцидентів, що підкреслює високий рівень кіберзагроз для країни [14].

На рис. 2.6 наведені сектори, які найбільше постраждали від хакерських атак в 2023 році в Україні.

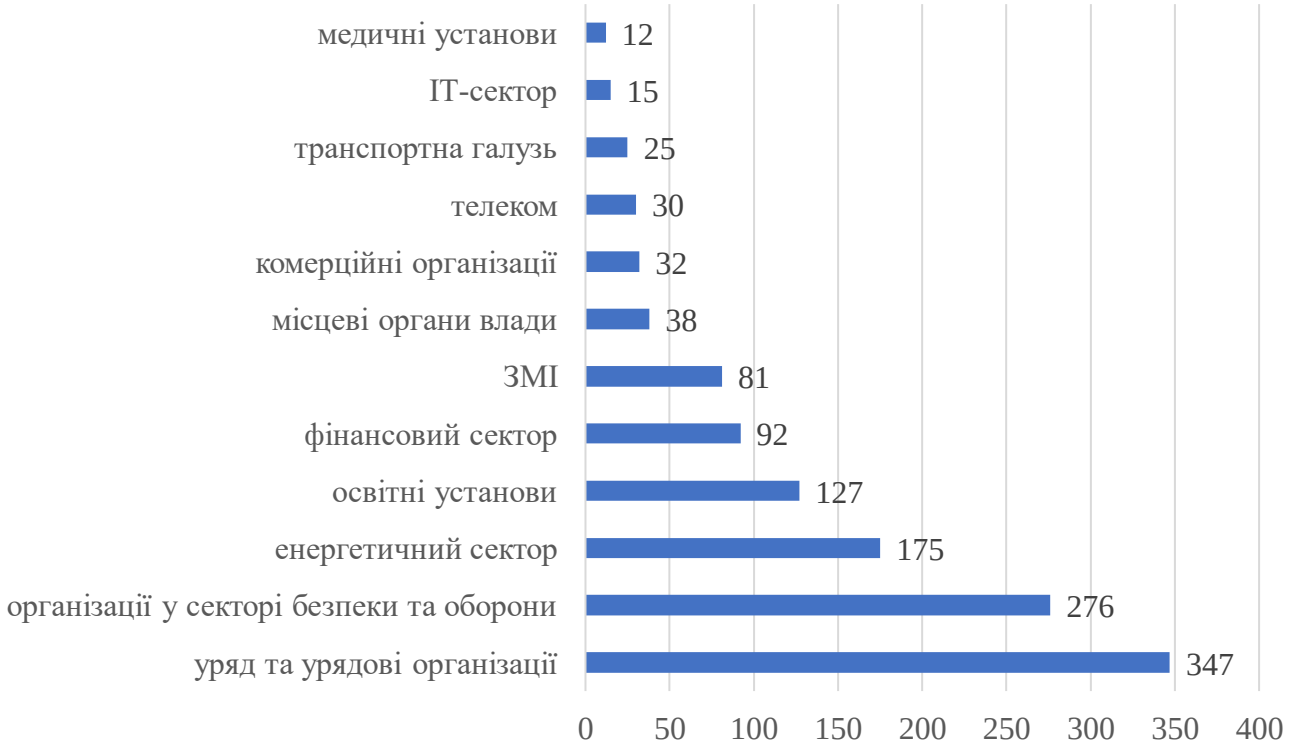

Рисунок 2.6 – Сектори, що найбільше постраждали від хакерських атак в Україні в 2023 році

Джерело: [53]

Згідно з даними, наведеними на рис. 2.6, основною мішенню кібератак у 2023 році стали урядові та місцеві органи влади, а також організації, що працюють

у секторі безпеки та оборони. Значна кількість атак була спрямована на енергетичний і телекомунікаційний сектори.

Протягом 2023 року за допомогою системи виявлення вразливостей і реагування на кіберінциденти (СВВ) було оброблено близько 18 мільярдів подій, що надійшли через системи моніторингу та передачі телеметричних даних про кібератаки. Під час первинного аналізу було виявлено 133 мільйони підозрілих подій у сфері інформаційної безпеки, а після додаткової фільтрації та вторинного аналізу було оброблено 148 тисяч критичних подій, які могли бути потенційними кіберінцидентами.

Загалом, аналітики безпеки зафіксували та обробили 1105 кіберінцидентів, що на 62,5% більше порівняно з 2022 роком. Також, у 2023 році до СВВ було підключено 24 нових об'єкти кіберзахисту з урядового, енергетичного та військового секторів [53].

Згідно з даними національних та міжнародних рейтингів, у 2023 році Україна посідала четверте місце в категорії «Національний індекс кібербезпеки», досягнувши рівня 81 %. За показником Глобального індексу кібербезпеки Україна займає 78-ме місце з рівнем 66 %. Індекс розвитку електронного урядування та Індекс мережевої готовності України становлять відповідно 46-е та 43-є місця з показниками 80 % і 55 %.

Хоча ці показники не є критично низькими, вони вказують на необхідність впровадження системи заходів щодо підвищення рівня захисту кіберпростору та удосконалення стратегій в цій сфері. Для поліпшення ситуації важливим кроком стане впровадження електронного урядування та розвиток інформаційних технологій, оскільки ці показники відкривають можливості для підвищення ефективності управління і розвитку інфраструктури, що є необхідними для забезпечення стабільності та безпеки в цих сферах [5].

Міжнародна співпраця є ключовим аспектом у зміцненні кібербезпеки України. Одним із важливих кроків у цьому напрямі стало створення нового механізму співробітництва в сфері кібербезпеки – «Талліннський механізм»,

оголошеного у 2023 році міністерствами закордонних справ України, Канади, Великої Британії, Сполучених Штатів Америки та країн Західної Європи.

Даний механізм націлений на покращення координації та надання підтримки Україні в захисті критичної інфраструктури від потенційних кіберзагроз, а особливо тих, що виникають через вплив російських кібероперацій, які стали частими у 2023 році. Враховуючи ці виклики, співпраця у рамках «Талліннського механізму» є важливою для зміцнення кіберзахисту України та надання довгострокової допомоги у протидії кіберзагрозам.

Цей проєкт має потенціал стати основною платформою підтримки для держав-членів, що активно сприяють розвитку цивільного кіберпотенціалу України та координації з іншими міжнародними організаціями, які також надають допомогу. Для забезпечення ефективного кіберзахисту України, союз країн-учасниць механізму пропонує підхід, що включає короткострокові, середньострокові та довгострокові стратегії, гарантуючи комплексне і стійке вирішення проблем кібербезпеки.

Ще одним значущим викликом для правового аспекту забезпечення кіберзахисту України є використання штучного інтелекту (ШІ) в галузі кібербезпеки, особливо в контексті національного та міжнародного законодавства. Незважаючи на його великий потенціал, лише 28 % організацій активно застосовують ШІ для забезпечення безпеки, хоча його використання здатне значно знизити витрати та прискорити процеси реагування на кіберзагрози.

За даними досліджень, організації, що активно використовують ШІ та автоматизацію в сфері кібербезпеки, зазвичай економлять в середньому 1,76 млн доларів США порівняно з тими, хто не застосовує ці технології. Це свідчить про значні переваги, які ШІ може принести в контексті зниження витрат і підвищення ефективності протидії кіберзагрозам, що є критичним для забезпечення кіберзахисту на рівні держави та в рамках міжнародної співпраці. Тому інтеграція ШІ в стратегії кібербезпеки потребує адаптації відповідного законодавства та нормативних актів, що забезпечать ефективне і безпечне використання цих технологій [13].

На сьогоднішній день у світі не існує єдиного законодавства, яке б чітко регулювало використання штучного інтелекту (ШІ) для захисту від кібератак, зокрема у контексті збереження та захисту конфіденційної інформації та персональних даних. Однак розробка такого законодавства є необхідною для визначення прав і обов'язків суб'єктів, які застосовують ШІ в кібербезпеці. Це включає створення механізмів відповідальності за порушення встановлених правил та стандартів. Подібні закони можуть встановлювати чіткі вимоги до використання ШІ у сфері кібербезпеки, зокрема для розробки та впровадження технологій захисту. Вони повинні також визначати стандарти безпеки та функціональності таких систем, щоб забезпечити їх ефективність та надійність. Законодавчі ініціативи також повинні враховувати захист прав громадян і організацій, гарантуючи відповідність міжнародним нормам та стандартам у сфері інформаційної безпеки. Таким чином, розвиток відповідного правового поля є ключовим етапом для забезпечення безпечного та етичного використання ШІ в кібербезпеці на глобальному рівні.

Отже, серед ключових передумов та чинників, які формують загрози кібербезпеці України, можна виділити такі:

– недосконаліть нормативно-правової бази, що часто є застарілою і не відповідає сучасним вимогам захисту інформації в умовах швидкої цифровізації;

– відсутність належної організаційної структури у багатьох державних органах, зокрема відсутність спеціалізованих підрозділів, необхідного кадрового забезпечення та ефективного контролю за кіберзахистом, що часто призводить до фінансування цих напрямів за залишковим принципом;

– необхідність створення механізмів розкриття інформації про вразливості в ситуації, коли всі сфери національного управління та діяльності стрімко цифровізуються, що ускладнює своєчасне виявлення потенційних загроз і реагування на них;

– невідповідність рівня підготовки спеціалістів сучасним вимогам, а також недостатньо ефективні механізми стимулювання та залучення фахівців до роботи в державному секторі, що знижує загальний рівень кібербезпеки;

– незавершеність впровадження організаційно-технічних моделей кіберзахисту, які відповідають новим типам загроз та зберігають актуальність у сучасних умовах;

– недостатня захищеність критичної інфраструктури та державних інформаційних ресурсів від кібератак, що є однією з основних проблем, яка потребує термінового вирішення для забезпечення національної безпеки.

Наведені фактори вказують на необхідність комплексного підходу до вдосконалення державної політики в сфері кіберзахисту, зокрема шляхом оновлення нормативно-правової бази, підвищення кваліфікації фахівців та розвитку відповідних інфраструктурних рішень.

Висновок до розділу 2

Сучасному інформаційному середовищу України притаманний суттєвий розвиток в межах вдосконалення нормативно-правового регулювання інформаційної безпеки, враховуючи значущість забезпечення інформаційної безпеки в стратегічних сферах державного управління.

Водночас забезпечення сталого управління кібербезпекою потребує розробки ефективних систем формування, обробки, поширення й захисту інформаційної інфраструктури, що сприятиме зростанню стійкості системи до актуальних загроз та викликів.

Одним з основних органів забезпечення криптографічного та технічного захисту інформаційних ресурсів є Державна служба спеціального зв’язку та захисту інформації, діяльність якої забезпечує стабільність зв’язку між державними органами й гарантує інформаційну безпеку на всіх рівнях державного управління та прийняття рішень.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1. Світовий досвід забезпечення інформаційної безпеки держави

Вивчення міжнародного досвіду забезпечення інформаційної безпеки є важливим кроком для вдосконалення цієї галузі в Україні. Оскільки країна перебуває в умовах гібридної війни та активно інтегрується в європейський інформаційний простір, необхідно адаптувати законодавство та практики співпраці між владою і громадськістю. Зростання рівня інформатизації та цифровізації суспільства збільшує ризики для безпеки державних і приватних даних.

Інформаційна безпека має стати частиною національної безпеки, тому важливо створювати ефективні механізми захисту від кіберзагроз та дезінформації. Окрім цього, потрібно активно працювати над підвищенням медіаграмотності та критичного мислення серед громадян, що допоможе протистояти інформаційним маніпуляціям [29].

Аналізуючи практики кібербезпеки в провідних країнах світу, можна зробити висновок, що наразі не існує єдиної уніфікованої моделі для створення національних систем кіберзахисту. Кожна країна адаптує свою стратегію залежно від особливостей національної інфраструктури, рівня загроз та політичних умов.

Інформаційна політика США реалізується на основі кількох ключових принципів, серед яких захист приватності, забезпечення безпеки і стабільності мереж, підтримка технологічних інновацій, координація державних зусиль, залучення приватних інвестицій, доступ до публічної інформації, реалізація принципу універсального доступу та покращення управління радіочастотним спектром [54].

Для забезпечення інформаційної безпеки країни відповідають кілька важливих державних установ, таких як Агентство національної безпеки (АНБ),

Національне управління кібербезпеки при Міністерстві внутрішньої безпеки, Федеральне бюро розслідувань (ФБР) та Центральне розвідувальне управління (ЦРУ). Робота АНБ спрямована на боротьбу з кіберзагрозами з боку неурядових мереж, активно співпрацюючи з приватним сектором та науковими установами. Дана співпраця передбачає заходи щодо захисту цивільних телекомунікаційних, банківських та електронних систем, а також спільну роботу з приватними організаціями і громадськими структурами у боротьбі з тероризмом [29].

З 2001 року питання інформаційної безпеки набуло пріоритетного значення у забезпеченні національної безпеки США та як наслідок призвело до запровадження низки федеральних ініціатив, спрямованих на захист національного інформаційного середовища в комп'ютерних мережах. Основна мета стратегії полягала у забезпеченні ефективного збору та аналізу даних розвідкою щодо зовнішніх загроз, які можуть виникати для інформаційної безпеки країни. Внаслідок цього розвинулася нормативно-правова база, спрямована на боротьбу з кіберзлочинністю. У 2003 році було впроваджено Національну стратегію безпечного кіберпростору як основу для подальших законодавчих ініціатив, зокрема, для розробки стандартів кібербезпеки та електронної аутентифікації [53].

З урахуванням досвіду США, для України є необхідність удосконалення національної системи інформаційної безпеки. Даний аспект включає створення ефективної системи реагування на інциденти в інформаційній сфері, імплементація комплексних заходів для зменшення загроз у кіберпросторі та покращення підготовки фахівців у сфері комп'ютерної безпеки. Також важливо забезпечити високу обізнаність населення щодо важливості захисту інформації та розвивати кооперацію, зокрема міжнародну, для забезпечення стійкої кібербезпеки [53].

США формують міжнародні принципи кібербезпеки, орієнтуючись на власні національні інтереси та індикатори. Однак, значна частина зусиль спрямована на вдосконалення внутрішньої політики. Так, Національна стратегія кібербезпеки США 2023 року визначає кілька ключових напрямів: захист

критичної інфраструктури, нейтралізація джерел загроз для інформаційної безпеки, розробка програм для підвищення безпеки та стійкості, інвестиції в майбутнє, налагодження міжнародного співробітництва та імплементація позитивного досвіду [15].

Крім того, США визнають, що забезпечення інформаційної безпеки неможливе в односторонньому порядку. Тому важливим аспектом їх стратегії є міжнародне партнерство. США прагнуть реалізувати кілька стратегічних ініціатив: заохочувати країни до посилення відповідальності за захист своїх інформаційних систем, створювати правовий режим для транскордонного доступу до інформації, формувати механізми колективної безпеки в рамках НАТО та інших міжнародних угод, а також зберігати свободу дій у інформаційному просторі для проведення інформаційних операцій [29].

Хоча це може виглядати як певний недолік у політиці США, їх підхід до міжнародної співпраці насправді підтверджує транснаціональний характер кіберзагроз, що вимагає спільних зусиль. Для України цей підхід є надзвичайно актуальним, адже боротьба з інформаційним тероризмом, спричиненим агресором, неможлива без підтримки міжнародних партнері.

У рамках Стратегії кібербезпеки Канади основними загрозами для національної безпеки визначені кібертероризм, кібершпигунство та кібервійна, зокрема ворожі дії інших держав у кіберпросторі. За координацію та реалізацію цієї стратегії, а також за вжиття заходів для протидії кіберзагрозам відповідає Міністерство громадської безпеки Канади [15].

У рамках євроінтеграції досвід забезпечення інформаційної безпеки країн ЄС є важливим для України. Європейський Союз розробив комплекс заходів, спрямованих на підвищення медіаграмотності та медіакультури серед громадян, створення систем попередження інформаційних загроз, а також на розвиток технологій захисту інформації. Крім того, ключовими аспектами є міжнародне співробітництво в галузі кібербезпеки, боротьба з кіберзлочинністю, протидія пропаганді, зокрема з боку росії, а також забезпечення захисту користувачів від онлайн-загроз. Ці ініціативи є основою діяльності держав-членів ЄС і мають

ціннісно-орієнтований характер, що сприяє зміцненню спільної безпеки в інформаційному просторі [55].

У рамках Європейського Союзу застосовується практика індивідуалізації окремих аспектів інформаційної безпеки, що дозволяє детально оцінювати загрози та розробляти відповідні методи і стратегії для їх нейтралізації. Як приклад можна навести Фінальний звіт дослідження кібербезпеки в енергетичному секторі, підготовлений компанією Blueprint Energy Solutions GmbH у 2019 році на замовлення Секретаріату Енергетичного Співтовариства ЄС. У документі підкреслюється вплив геополітичних факторів на рівень кібербезпеки в енергетичній галузі. Крім того, зазначено, що для зменшення ризиків необхідно усунути прогалини в нормативно-правових актах і в інституційних структурах, що відповідають за кібербезпеку в енергетиці. Для України така індивідуалізація є важливим позитивним досвідом, оскільки вона дає змогу диференціювати загрози та визначати конкретні напрямки для їх ефективної протидії [8].

У Великій Британії захист критичної інфраструктури та мінімізація загроз її стабільному функціонуванню, особливо від терористичних атак, покладаються на Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). У березні 2013 року був створений Центр протидії кібернетичним загрозам, основними завданнями якого є запобігання та швидку нейтралізацію кіберзагроз на об'єкти критичної інфраструктури [15].

Згідно зі стратегією кібербезпеки Австрії, центральним органом у цій сфері визначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ, що не тільки виконує функції правоохоронного органу, а й координує заходи боротьби з кіберзлочинністю та забезпечення кібербезпеки в країні [15].

Агентство внутрішньої безпеки Польщі (АВБ), яке відповідає за контррозвідувальну діяльність, має центральне значення у забезпеченні кібербезпеки країни. У 2013 році АВБ розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної

оборони. Даний підрозділ відповідає за захист інформаційних систем, кібероборону та реалізацію наступальних кібероперацій у межах активного кіберзахисту [56].

Правова база політики інформаційної безпеки в Польщі включає ряд законів, що визначають ключові напрямки в інформаційній сфері, регулюють стандарти для технологій інформаційного зв'язку та визначають порядок залучення іноземних інвестицій, сертифікацію інформаційної діяльності. Додатково окреслені права релігійних організацій, зокрема католицької церкви, щодо здійснення інформаційної діяльності, створення комп'ютерних мереж і систем електронного зв'язку [29].

Задля протидії інформаційним загрозам Польща активно залучає громадянське суспільство. Так, у 2017 році був створений Центр аналізу пропаганди та дезінформації, основною метою якого є ідентифікація та нейтралізація російської дезінформації в медіапросторі Польщі. Варто відзначити, що досвід Польщі, хоча й схожий на український, має важливу перевагу: це активне залучення громадян до боротьби з інформаційними загрозами, розробка ефективних механізмів протидії пропаганді та стандартизація надання інформаційних послуг[29].

Стратегія інформаційної безпеки Федеративної Республіки Німеччина фокусується на десяти основних напрямках: захисті критично важливих інформаційних інфраструктур, забезпеченні безпеки IT-систем у країні, посиленні інформаційної безпеки в органах державного управління, створенні національної ради з кібербезпеки, боротьбі з кіберзлочинністю, а також на координації дій для забезпечення безпеки на рівні Європи. Стратегія також передбачає використання надійних технологій, розвиток компетенцій персоналу у федеральних установах і захист особистих даних громадян під час обміну електронною поштою. Ця стратегія поєднує два основні аспекти: національний і міжнародний. На національному рівні вона включає механізми внутрішньої протидії інформаційним загрозам, а на міжнародному забезпечує процес співпраці та координації з європейськими інституціями для посилення

колективної безпеки. Такий комплексний підхід, з акцентом на деталізацію конкретних сфер інформаційної безпеки, дозволяє ефективно захищати національні інтереси Німеччини [15].

Досвід Ізраїлю в галузі кібербезпеки є особливо важливим для України, оскільки Ізраїль, незважаючи на обмежені природні ресурси та постійні військові загрози, зосередив свої зусилля на розвитку науково-технологічного потенціалу, ставши одним з лідерів у сфері інновацій. Відсутність сировинних ресурсів та необхідність забезпечення національної безпеки стимулювали Ізраїль до значних досягнень у медичних та інформаційних технологіях, де країна здобула визнання на світовому рівні. Протягом 75 років, проживаючи в умовах постійної терористичної загрози, ізраїльтяни розвивали культуру безпеки, забезпечуючи стабільність і захист держави. Кібербезпека стала одним з основних пріоритетів для Ізраїлю, який є однією з найбільш комп'ютеризованих країн на Близькому Сході [57].

Ізраїль активно нарощує інвестиції в сферу кібербезпеки, займаючи 15% від світового обсягу вкладень у цю галузь. Ключова концепція ізраїльської кібербезпеки полягає в поєднанні новітніх технологій із створенням правових механізмів, спрямованих на захист інформаційної інфраструктури. Оскільки сучасні кіберзагрози потребують комплексного підходу, це вимагає не лише національних, але й міжнародних стратегій для гарантування безпеки, що акцентує важливість глобального регулювання кіберпростору. Мілітаризація кіберпростору ставить нові виклики, оскільки атаки на критичну інфраструктуру можуть спричинити непередбачувані наслідки. Для мінімізації цих загроз провідні держави активно обговорюють питання на різних рівнях і розробляють інтегровані стратегії, що поєднують як національні, так і міжнародні заходи [57].

Ізраїльська кібербезпекова інфраструктура включає понад 450 компаній, серед яких виділяються відомі підприємства та інвесторів в сферу кіберзахисту: «Check Point», «Jerusalem Venture Partners (JVP) Cyber Labs» тощо. Окрім цього, важливим елементом є науково-дослідні ініціативи, що сприяють тісній співпраці між технологічними компаніями та дослідницькими установами [58].

Законодавче регулювання інформаційної безпеки в Ізраїлі ґрунтується на комплексному наборі нормативно-правових актів, що охоплюють як основні закони, так і численні підзаконні акти, включаючи постанови Міністерства юстиції та урядові рішення. Окрім того, значну роль у розробці політики відіграють правила, які визначають неурядові організації, що регулюють надання інтернет-послуг. Така нормативна база забезпечує належний захист як для користувачів інформаційних послуг, так і для національної безпеки, одночасно зберігаючи права на свободу інформації. Водночас органи, що мають доступ до інформації, зокрема правоохоронні та розвідувальні структури, повинні дотримуватися принципів прозорості та відповідальності перед громадськістю [57].

Досвід Ізраїлю у створенні ефективної системи кібербезпеки має велике значення для України, зокрема в умовах нинішнього конфлікту з Росією. Подібно до Ізраїлю, Україна перебуває в постійному стані готовності до загроз національній безпеці, що вимагає впровадження комплексних підходів до захисту кіберпростору. Ізраїль успішно поєднує правові, організаційні та технологічні заходи в сфері кібербезпеки, зокрема створення спеціалізованих кіберпідрозділів і координаційних центрів. Важливою складовою цього підходу є активне залучення як державних, так і приватних структур, а також міжнародна співпраця для забезпечення кіберзахисту. Для України, яка стикається з постійними кіберзагрозами, ізраїльська модель може бути корисною при розбудові власної системи кібербезпеки. Реалізація подібних стратегій і структур допоможе зміцнити здатність України протидіяти кіберзлочинності та захищати національні інтереси в цифровому просторі [58].

Зарубіжний досвід у сфері забезпечення інформаційної безпеки має багато унікальних аспектів, які значною мірою визначаються специфічними умовами кожної країни. Ключовими факторами, що впливають на формування цієї системи, є такі:

1. Розвиток інформаційного суспільства, таких як зростання імплементації інформаційних технологій у сфери громадського життя, що

безпосередньо впливає на рівень захисту інформації. Чим більше технології інтегровані в суспільні процеси, тим складнішим є управління інформаційною безпекою.

2. Інтеграція в міжнародні структури – країни, які є членами таких організацій, як Європейський Союз чи НАТО, мають більший доступ до міжнародних стандартів безпеки та співпрацюють з іншими державами для вирішення спільних загроз у кіберпросторі.

3. Позиціонування інформаційної безпеки в національній системі безпеки, а також створення відповідних внутрішніх механізмів, здатних адаптуватися до нових викликів.

4. Нормативно-правове оформлення принципів інформаційної безпеки – це розробка законодавчих актів і стандартів, які регулюють безпеку інформації, визначаючи її основні рівні та способи забезпечення.

5. Правовий статус інформації – в кожній країні існують свої підходи до визначення прав і обов'язків у сфері інформаційної безпеки, що залежать від її конституційних норм і розуміння права на інформацію, що може варіюватися від однієї держави до іншої [54].

Таким чином, кожен з цих факторів є важливим для формування національної політики та практик у сфері інформаційної безпеки, враховуючи унікальність політичних, правових та технологічних умов кожної країни.

Отже, можна зазначити, що досвід інших країн у забезпеченні інформаційної безпеки є важливим для України, особливо в контексті створення національного інформаційного простору. Це включає розвиток механізмів попередження загроз, наукове обґрунтування цих загроз, а також формування ефективної системи громадського інформаційного управління. Крім того, важливим аспектом є створення спеціалізованих інституцій, які забезпечуватимуть захист національних інтересів в інформаційній сфері.

3.2. Напрями вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації

Зі стрімким розвитком новітніх інформаційних технологій існує потреба в постійному вдосконаленні того, як державні установи захищають свої інформаційні ресурси, а також у вдосконаленні інструментів і програмного забезпечення для забезпечення інформаційної безпеки. Недостатня ефективність і застарілість існуючих механізмів управління інформаційною безпекою, а також відсутність перевірених наукових методів і технічних рішень для їх удосконалення можуть мати серйозні негативні наслідки як для нації, так і для її громадян.

Інформаційна складова є важливим компонентом війни російської федерації проти України, що створює суттєві загрози національній безпеці. В умовах агресії спостерігається цілеспрямоване знищення інформаційної інфраструктури тимчасово окупованих територій, проведення кібератак проти України та блокування каналів для поширення актуальної інформації про суспільно-політичну ситуацію в країні. Окрім того, в умовах активної пропагандистської кампанії проти України проводяться деструктивні інформаційні операції. З огляду на швидкий розвиток інформаційного суспільства та глобалізацію інформаційного простору, а також масове застосування інформаційно-комунікаційних технологій у різних сферах життя, питання інформаційної безпеки набувають надзвичайної актуальності [18].

Для ефективного вирішення стратегічних завдань у сфері інформаційної безпеки України необхідно розробити комплексну стратегію, яка охоплюватиме всі сфери суспільства, зокрема державні структури, громадянське суспільство та бізнес. Для цього слід створити національні центри аналізу та реагування, які будуть здійснювати моніторинг, аналіз та оперативну реакцію на кіберзагрози і нові вектори атак. Крім того, потрібно вдосконалити заходи кібербезпеки для захисту критичних об'єктів інфраструктури. З метою попередження можливих кібератак необхідно забезпечити безперервний моніторинг та аналіз нових

тенденцій у сфері кібербезпеки для своєчасного виявлення і нейтралізації загроз, а також розробити та адаптувати законодавчу базу в цій галузі до сучасних викликів і міжнародних стандартів [5].

Для ефективного створення адаптивної моделі національної інформаційної політики, яка відповідатиме різним умовам, зокрема умовам воєнного стану, державі та громадянському суспільству необхідно зосередитися на таких ключових напрямках (рис.3.1).

Рисунок 3.1 – Ключові напрямки створення адаптивної моделі національної інформаційної політики

Джерело: [65]

Окремо розглянемо рекомендації щодо забезпечення інформаційної безпеки України в зовнішньополітичній сфері є:

– розробка стратегічних напрямків державної політики для вдосконалення інформаційного забезпечення зовнішньополітичного курсу України;

– розробка та реалізація комплексу заходів щодо посилення інформаційної безпеки інфраструктури органів управління, що відповідають за реалізацію зовнішньої політики України, а також забезпечення інформаційної безпеки представництв та організацій України за кордоном;

– створення умов для ефективної боротьби з дезінформацією, що поширюється за кордоном щодо зовнішньої політики України, через діяльність українських представництв та організацій;

– вдосконалення інформаційного забезпечення для протидії порушенням прав і свобод українських громадян та юридичних осіб за кордоном;

– покращення інформаційного забезпечення суб'єктів України, які займаються питаннями зовнішньополітичної діяльності, з урахуванням їх компетенції [59].

При розробці сучасної національної інформаційної політики доцільно передбачити фінансування технологічної інфраструктури країни та підготовку громадян до правильного використання інформації. Одночасно має бути розроблений відповідний законодавчий механізм для регулювання цієї діяльності.

Система забезпечення інформаційної безпеки виступає основним елементом на шляху досягнення національної безпеки. Ключовими завданнями цього механізму є:

– виявлення потенційних зовнішніх й внутрішніх загроз інформаційній безпеці країни;

– встановлення показників інформаційної безпеки, їх аналіз та співставлення зі встановленими нормативами;

– створення та впровадження системи моніторингу загроз, яка охоплює отримання, опрацювання, збереження і аналіз даних;

– розробка комплексу заходів, спрямованих на забезпечення стабільності і захисту системи інформаційної безпеки країни [60].

Під час воєнного стану інформаційна зброя стає потужним інструментом ведення війни завдяки своїй технічній інноваційності, силі та непомітності, що робить її надзвичайно небезпечною. У зв’язку з цим інформаційна безпека України повинна ґрунтуватися на злагоджених діях державних органів і громадянського суспільства. В умовах війни особливо важливим є підвищення рівня інформаційної культури серед населення, що дозволяє ефективніше протистояти інформаційним атакам та зміцнювати суверенітет країни [59].

Забезпечення доступу до інформації є ключовим елементом демократичного процесу в Україні. В умовах повномасштабної війни одним із головних завдань держави є гарантування принципів верховенства права, що включають доступ до публічної інформації. Проте в умовах воєнного стану міркування національної безпеки вимагають, щоб відомство, відповідальне за знищення публічної інформації, могло приймати рішення про обмеження доступу до певної інформації та дотримуватися обмежень, встановлених законом. Тому важливо в процесі формування та реалізації державної інформаційної політики знаходити баланс між гарантуванням конституційного права на вільне отримання та поширення інформації та необхідними обмеженнями в інтересах національної безпеки [61].

В умовах воєнного стану доступ до публічної інформації набуває критичної важливості, адже він є потужним правовим інструментом, здатним рятувати життя та зберігати здоров'я громадян. Надання швидкої та завчасної інформації населенню про ризик нападу чи окупації дозволить своєчасно евакуюватись і запобігти гуманітарним катастрофам, злочинам проти людяності та навіть геноциду з боку російських військ.

Водночас, в умовах інтенсивної інформаційної війни, спричиненої дезінформацією з боку спеціальних служб противника, а також жорстокими діями російських військових на українській території, важливо дотримуватися балансу. З одного боку, потрібно забезпечити можливість громадян вільно висловлювати свої погляди та отримувати достовірну інформацію, з іншого – систематично захищати життя та здоров'я осіб [62].

Загальним правилом є обов'язкове оприлюднення публічної інформації без затримок, але не пізніше п'яти робочих днів після затвердження документа. Однак, у контексті введення в Україні правового режиму воєнного стану, об'єм повноважень та компетенція окремих розпорядників інформації можуть зазнавати значних змін. Це може передбачати встановлення обмежень з боку уповноважених органів відповідно до статті 8 Закону України «Про правовий режим воєнного стану». Водночас такі обмеження не можуть поширюватися на інформацію щодо нормативно-правових актів, що стосуються обмеження конституційних прав і свобод, а також на дані про стан навколишнього середовища та якість харчових продуктів [62].

Ураховуючи обмеження, встановлені в умовах воєнного стану, реалізація права на доступ до публічної інформації здійснюється переважно через ознайомлення громадян з інформацією, доступною в відкритих джерелах Інтернету.

В таких умовах постає важливе питання реалізації превентивних заходів, що мають здійснювати компетентні органи для охорони інформації з обмеженим доступом. Одним з таких заходів може бути підвищення кваліфікації державних службовців з питань інформаційної безпеки. У деяких випадках, коли існує підозра, що запитувана інформація може бути використана в інтересах ворога, розпорядники інформації мають право негайно направляти копії запитів до Служби безпеки України для проведення перевірки осіб, які збирають таку інформацію [63].

Розглядаючи шляхи інтеграції міжнародного досвіду в забезпечення інформаційної безпеки в Україні, можна виділити такі основні напрямки:

1. Адаптація міжнародних стандартів, зокрема ISO/IEC 27001, що окреслює та уніфікує вимоги до створення та підтримки системи управління інформаційною безпекою, а також виступає механізмом постійного її вдосконалення.

2. Розширення міжнародного співробітництва. Активне співробітництво з міжнародними організаціями, такими як ЄС, НАТО та ООН, дозволить Україні обмінюватися інформацією щодо кіберзагроз, обирати кращі практики та спільно розробляти рішення для протидії кіберзлочинності. Можливими засобами протидії

кіберзлочинності в даному секторі можуть виступати спільні навчання з міжнародними партнерами, участь в міжнародних ініціативах з кібербезпеки тощо.

3. Удосконалення законодавства. Для забезпечення ефективного захисту інформації важливо оновити національне законодавство, враховуючи міжнародний досвід. Даний механізм включає як адаптацію існуючих законів, так і розробку нових нормативних актів, які виступають законодавчим фундаментом захисту інформації як в державному, так і в приватному секторах.

4. Розвиток державно-приватного партнерства. Співпраця між державою і приватним сектором є важливим елементом у забезпеченні інформаційної безпеки. Спільні зусилля в обміні інформацією про кіберзагрози та розробці технологічних рішень допоможуть ефективно реагувати на загрози та впроваджувати інноваційні методи захисту інформації.

5. Доступ до сучасних інформаційних технологій, включаючи підтримку інфраструктури та модернізацію державних і приватних інформаційних систем.

6. Впровадження сучасних технічних засобів захисту, таких як шифрування даних, міжмережеві екрани та системи виявлення й попередження вторгнень, які забезпечують захист від кіберзагроз та допомагають зберігати конфіденційність інформації.

Отже, в сучасних умовах, з огляду на тривалу війну та агресивні дії російської федерації, забезпечення інформаційної безпеки є однією з головних пріоритетних завдань для України. Серед основних викликів – це кіберзагрози, інформаційна війна, технологічні труднощі та психологічний вплив на громадян. Для ефективної протидії загрозам необхідно застосовувати комплексний підхід, який включає оновлення системи кіберзахисту, розробку стратегій боротьби з дезінформацією, модернізацію технічної інфраструктури та підвищення стійкості населення до маніпуляцій. Тільки спільні зусилля державних органів, громадянського суспільства та міжнародних партнерів можуть забезпечити належний рівень захисту інформаційного простору України та сприяти зміцненню національної безпеки й суверенітету.

3.3. Перспективи розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів

Експерти провідних компаній у сфері кіберзахисту дійшли висновку, що для мінімізації ризиків кібератак та витоків даних, а також для забезпечення максимальної ефективності інвестицій у кібербезпеку, необхідно використовувати надійні системи захисту кінцевих пристроїв з функціями виявлення загроз і швидкого реагування на них.

На основі дослідження, проведеного компанією Hikvision, можна виділити такі ключові тенденції у сфері кібербезпеки:

– швидкий розвиток штучного інтелекту з інтеграцією технологій Інтернету речей та ШІ;

– розвиток хмарних технологій та перехід від традиційних систем зберігання даних до конвергентних рішень;

– поширення біометричних технологій для контролю доступу;

– запровадження моделей Zero Trust, що базуються на принципах мінімальної довіри та максимальної перевірки.

Ці тренди відображають сучасні виклики та можливості у сфері кібербезпеки, спрямовані на підвищення стійкості систем до загроз [64].

Штучний інтелект (ШІ) має суттєву можливість видозмінити звичні аспекти людського життя, що можна порівняти з революційними зрушеннями, спричиненими розвитком Інтернету з початку XXI століття. Ці трансформації вже змінили економічні структури, суспільні процеси, політичну динаміку та повсякденне життя. Хоча ШІ ще не набув повсюдного застосування, у всьому світі тривають активні дискусії про способи регулювання його впливу на такі сфери, як праця, охорона здоров’я, освіта, розваги та інші аспекти людської діяльності [64].

Обговорення ШІ зосереджено не стільки на термінах чи інтенсивності змін, скільки на тому, як його вплив може трансформувати саму природу біологічного існування та глобальний світопорядок. Важливо підкреслити, що ШІ не лише

модифікує процеси виконання господарської, соціальної чи державної діяльності, але й змінює способи досягнення кінцевих результатів, оскільки дозволяє автоматизувати завдання, традиційно виконувані людиною. Таким чином, основна трансформація полягає у заміні людського фактору, що відкриває нові горизонти, але водночас ставить перед людством серйозні виклики [65].

Аналізуючи досвід використання штучного інтелекту (ШІ) в національній інформаційній безпеці США, можна запропонувати кілька напрямів адаптації цієї технології в Україні:

1. Аналіз технології та стратегічне планування. Провести дослідження процесів застосування ШІ, зокрема аналіз його можливостей і загроз. Розробити документ, що визначатиме перспективи використання ШІ в Україні, включаючи підходи до його регулювання, очікувані результати та національну стратегію розвитку технологій ШІ.

2. Законодавче забезпечення. Розробити та впровадити нормативно-правову базу, яка регулюватиме діяльність у сфері ШІ, забезпечуватиме захист від ризиків і створюватиме умови для його розвитку. Законодавство має враховувати міжнародні стандарти, адаптуючи їх до національних потреб.

3. Діалог із суспільством і бізнесом. Організувати систематичну взаємодію між державними органами, громадянським суспільством і бізнесом. Це дозволить визначити прийнятні межі використання ШІ в різних сферах, зокрема у військовій, економічній, соціальній та освітній діяльності.

4. Освітньо-інформаційна діяльність. Використовувати сучасні медіа-технології для інформування громадськості про потенційні ризики та загрози, зокрема щодо дезінформації, створюваної за допомогою ШІ. Роз’яснювальна робота сприятиме підвищенню інформаційної грамотності та протидії маніпуляціям.

5. Контроль у стратегічно важливих сферах. В умовах воєнного стану варто застосовувати ШІ з особливою обережністю в стратегічних галузях держави, таких як оборона, енергетика, інфраструктура та кібербезпека. До створення чітких

алгоритмів використання ШІ важливо мінімізувати ризики витоку чи несанкціонованого доступу до чутливої інформації [65].

Імплементація цих підходів допоможе Україні інтегрувати технології ШІ у національну систему безпеки та розвивати її з урахуванням викликів сучасного світу. Зростаюча стурбованість щодо стрімкого розвитку штучного інтелекту (ШІ) спричинила активізацію досліджень, присвячених правовим наслідкам його використання. Хоча переважна більшість таких досліджень зосереджується на аналізі впливу ШІ у приватному секторі, зокрема на права окремих осіб, не менш важливим є вивчення ризиків, які виникають при застосуванні ШІ у сфері державного управління [65].

Використання ШІ в урядових структурах може мати суттєвий вплив на функціонування публічної влади, інформаційну безпеку держави, а також на права та свободи громадян. Основними викликами є забезпечення прозорості й підконтрольності алгоритмів ШІ, запобігання зловживанням і помилкам у прийнятті рішень, а також захист особистих даних і гарантування дотримання прав людини.

Аналіз цих аспектів є ключовим для створення ефективної нормативно-правової бази, яка забезпечить безпечне та етичне використання ШІ в державному управлінні, зберігаючи баланс між інноваціями та дотриманням прав громадян [64].

Дослідники штучного інтелекту (ШІ) наголошують, що ця технологія постійно залишається на передовій проривних інновацій завдяки своїй надзвичайній здатності до трансформації у різних сферах – від промисловості та сільського господарства до охорони здоров’я та оборони. Особливо значущим є вплив ШІ на національну інформаційну безпеку, що викликає все більше занепокоєння [28].

Розширення використання ШІ створює нагальну потребу у розробці нормативно-правових актів і регуляторних механізмів для забезпечення безпеки інформаційних систем на національному рівні, як це практикується у США та країнах ЄС. Особливі виклики виникають, коли ШІ застосовується в процесах прийняття урядових рішень, які передбачають здійснення владних повноважень

або вплив на права громадян. Наприклад, це може стосуватися нормотворчої діяльності (регуляторний аналіз), судових рішень (надання грантів чи допомоги) або примусового виконання (інспекції чи перевірки) [65].

Водночас ШІ демонструє високу ефективність у внутрішньому управлінні державними процесами, взаємодії з громадськістю (наприклад, через чат-боти), моніторингових завданнях і наданні державних послуг. Однак, впроваджуючи ці інструменти, важливо ретельно зважувати потенційні вигоди й ризики, аби уникнути шкоди, насамперед, для інформаційної безпеки держави, яка є однією з найбільш чутливих до впливу ШІ сфер. Застосування штучного інтелекту (ШІ) у процесі прийняття державних рішень, особливо тих, що стосуються механізмів національної безпеки, потребує особливої уваги до його ролі в цих процесах. Вирішальним є питання: чи стане ШІ інструментом, який лише підтримує прийняття рішень, чи буде він здатний повністю замінити працівників органів публічної влади та адміністрацій? Відповідь на це питання є критичною, адже автономність таких систем може становити серйозний ризик для національної, зокрема інформаційної, безпеки.

Серед основних ризиків, пов’язаних із використанням ШІ у сфері національної інформаційної безпеки, ключовим є здатність системи діяти незалежно від людського контролю. Якщо алгоритми ШІ матимуть можливість встановлювати правила та самостійно приймати рішення, це може суттєво вплинути на безпеку держави. Виникає також проблема узгодження таких дій із принципами публічного права, зокрема щодо відповідальності перед громадськістю [65].

Додатковий виклик полягає у забезпеченні прозорості роботи систем ШІ. Громадяни повинні бути заздалегідь поінформовані про потенційні сценарії використання цих технологій, особливо в умовах критичних подій, таких як початок ядерної війни або масштабні природні чи космічні катаклізми. Невизначеність у таких питаннях може призвести до зниження довіри до державних інститутів та створити додаткові ризики для національної стабільності [65].

В Україні спостерігається активний розвиток штучного інтелекту (ШІ) у промисловості, медицині, ОПК та інформаційній безпеці. Досвід США та Європи став основою для створення у 2020 році Концепції розвитку штучного інтелекту, яка визначає цілі, завдання та терміни впровадження ШІ. Вона трактує ШІ як технологію, здатну виконувати складні завдання за допомогою наукових методів та алгоритмів.

В 2023 році відновлено роботу Комітету з питань розвитку ШІ при Міністерстві цифрової трансформації, який працює над регламентом використання ШІ, включаючи питання дезінформації.

Аналіз використання ШІ в національній інформаційній безпеці США дозволяє запропонувати такі напрямки застосування цієї технології в Україні:

– провести дослідження та підготувати документ, що окреслить очікування щодо впровадження ШІ, регулювання технології та прогнозовані результати;

– розробити законодавчу базу для регулювання та розвитку ШІ;

– організувати діалог із громадянським суспільством і бізнесом щодо меж використання ШІ у різних сферах;

– здійснювати інформаційно-просвітницьку діяльність через медіа, зосереджену на запобіганні дезінформації, пов’язаній із ШІ.

У стратегічно важливих сферах під час війни застосовувати ШІ з обережністю, уникати ризику витоку даних до створення надійних алгоритмів безпеки [65].

Перспективи використання хмарних технологій та перехід від традиційних систем зберігання даних до конвергентних рішень для розвитку кіберзахисту державних інформаційних ресурсів є значними, оскільки ці технології забезпечують вищу ефективність, гнучкість та безпеку. Хмарні платформи дозволяють централізувати управління даними, що спрощує моніторинг, доступ і контроль за інформацією, особливо для великих державних установ з численними розрізненими ресурсами. Це значно покращує управління даними та забезпечує цілісність інформаційної системи.

Крім того, хмарні технології підтримують інтеграцію з різними системами безпеки, що включають багаторівневий захист, шифрування даних та автоматичне оновлення безпеки. Це створює додаткові гарантії для захисту від кіберзагроз і знижує ймовірність витоків або втрати даних. Хмарні рішення також забезпечують ефективне резервне копіювання та швидке відновлення даних у разі інцидентів, що важливо для забезпечення безперервності функціонування критичних систем державної інформаційної безпеки [11].

Використання хмарних технологій також дає змогу знижувати витрати на підтримку фізичних серверів і обладнання, оскільки в хмарі можна адаптувати обсяг зберігання та обчислювальних потужностей залежно від поточних потреб. Це дозволяє значно зменшити фінансові витрати на інфраструктуру, а також оптимізувати енергоспоживання. Крім того, хмара надає можливість інтеграції з сучасними цифровими інструментами, такими як аналітика даних, штучний інтелект і автоматизація, що підвищує ефективність аналізу і прийняття рішень у сфері кіберзахисту.

Незважаючи на всі переваги, перехід до хмарних технологій вимагає вирішення деяких викликів, таких як забезпечення суверенітету даних, удосконалення нормативно-правового регулювання, навчання персоналу та вибір надійних постачальників послуг. Однак у довгостроковій перспективі цей перехід є важливим кроком у зміцненні кібербезпеки та оптимізації державних інформаційних систем.

Поширення біометричних технологій для контролю доступу є важливим етапом у розвитку систем безпеки, оскільки ці технології використовують унікальні фізичні або поведінкові характеристики індивіда, такі як відбитки пальців, розпізнавання обличчя, сітківка ока або голосові зразки. Це забезпечує високий рівень ідентифікації, оскільки біометричні дані важко підробити або змінити, що робить їх надійнішим способом аутентифікації порівняно з традиційними методами, такими як паролі чи картки доступу [64].

Проте, впровадження біометричних технологій також передбачає необхідність забезпечення відповідного рівня захисту цих даних. У зв'язку з цим

постає питання етики, приватності та законодавчого регулювання використання біометрії, оскільки збір та зберігання біометричних даних можуть порушувати права громадян щодо конфіденційності.

Запровадження моделей Zero Trust в сфері кібербезпеки є однією з найбільш перспективних стратегій для захисту інформаційних систем і даних в умовах сучасних кіберзагроз. Модель Zero Trust передбачає, що жоден користувач, пристрій чи система не довіряються за замовчуванням, навіть якщо вони знаходяться в межах корпоративної мережі. Всі запити на доступ до ресурсів повинні проходити ретельну перевірку, незалежно від того, чи є користувач зовнішнім чи внутрішнім. Це суттєво змінює традиційний підхід до безпеки, який зосереджувався на захисті периметра мережі, і вводить нові принципи для управління доступом [64].

Ключовим елементом Zero Trust є верифікація на кожному етапі взаємодії користувача з системою. Для цього використовуються різноманітні методи автентифікації, такі як багатоетапна аутентифікація (MFA), біометричні дані, поведінкові аналітики та інші технології, що дозволяють точно визначити, хто запитує доступ і на яких умовах. Крім того, модель Zero Trust передбачає постійний моніторинг і оцінку ризиків, що дозволяє оперативно реагувати на будь-які зміни в поведінці користувачів або систем [64].

Однією з головних переваг цієї моделі є здатність мінімізувати можливості для внутрішніх атак і зменшити шкоду від компрометації одного елементу системи. У традиційних моделях безпеки порушення периметра могли залишати значні частини мережі вразливими, що спрощувало можливість зловмисникам отримати доступ до важливих даних. В межах роботи системи Zero Trust кожен доступ до ресурсів оцінюється окремо, що значно знижує ймовірність успішної атаки [56].

Зазначимо, що впровадження Zero Trust потребує значних інвестицій у технології та інфраструктуру. Це включає оновлення існуючих систем автентифікації, впровадження інструментів моніторингу та аналізу, а також перепідготовку співробітників для роботи в нових умовах. Крім того, для успішного впровадження Zero Trust необхідне тісне співробітництво між IT-

відділом, відділом безпеки та іншими підрозділами організації, щоб забезпечити комплексний підхід до захисту даних.

Отже, перспективи розвитку кіберзахисту державних інформаційних ресурсів сприяють інтеграції сучасних цифрових технологій, таких як штучний інтелект, хмарні обчислення, біометричні системи та моделі Zero Trust. Вони дозволяють значно покращити рівень безпеки завдяки автоматизації процесів моніторингу, оперативному виявленню загроз та забезпеченню гнучкої ідентифікації доступу. Використання цих інструментів дозволяє державним установам ефективно протистояти новим кіберзагрозам, знижуючи ризики витоку інформації та зловмисних атак. Водночас важливо забезпечити належний контроль і регулювання використання таких технологій, щоб мінімізувати потенційні ризики для національної безпеки.

Висновок до розділу 3

Врахування особливостей міжнародного досвіду в процесі забезпечення системи інформаційної безпеки є суттєвим елементом вдосконалення інформаційної безпеки України, оскільки даний аналіз дозволяє більш широко розглянути процеси в межах системи реагування на існуючі загрози, забезпечення громадського інформаційного простору, організації та роботи спеціалізованих інституцій щодо захисту національних інтересів в інформаційній сфері.

Кризові виклики сучасності, зокрема деструктивний характер військових дій та інформаційних впливів з боку росії наразі виступають основними загрозами національної безпеки. Водночас ефективним засобом протидії слугує комплексний підхід до реагування та протидії кіберзлочинності та інформаційному впливу, що потребує реалізації на державному рівні, а також завдяки активній міжнародній співпраці та громадянському впливу.

ВИСНОВКИ

У кваліфікаційній роботі розкрито теоретичні та практичні аспекти кіберзахисту державних інформаційних ресурсів в Україні. В ході дослідження, нами було досягнуто визначених у роботі мети та завдань.

1. Розкрито поняття державних електронних інформаційних ресурсів, відповідно до якого визначено, що кібербезпека є ключовим інструментом регулювання кіберпростору, що водночас виступає важливим елементом системи національної безпеки держави. Кіберзахист державних інформаційних ресурсів є основою національної безпеки, оскільки він гарантує стабільність та захищеність критично важливих інформаційних систем від кіберзагроз.

Державні електронні інформаційні ресурси відіграють ключову роль у модернізації державного управління в Україні, забезпечуючи ефективну інтеграцію інформації та автоматизацію процесів. Важливою проблемою залишається термінологічна несумісність у різних законодавчих актах, що ускладнює використання інформаційних ресурсів. Водночас для забезпечення максимальної ефективності в роботі державних електронних послуг, важливо перейти від паперових форм до повністю автоматизованої електронної взаємодії. Загалом розвиток та вдосконалення національних електронних інформаційних ресурсів є невід’ємною частиною сучасної цифрової економіки та сприяє забезпеченню прозорості та доступності державних послуг для населення.

2. Визначено сутність та роль кіберзахисту державних інформаційних ресурсів, значення якого полягає у забезпеченні ефективного кіберзахисту дозволяє зберегти конфіденційність, цілісність і доступність даних, що є необхідними для функціонування державних органів, економіки та інфраструктури.

Основним стратегічним завданням інформаційної безпеки в Україні є формування потужного національного інформаційного простору, який виступає важливим елементом, що підтверджує присутність держави на світовій інформаційній арені. Реалізація цієї місії передбачає побудову ефективних систем

протидії всім інформаційним загрозам, захист інформаційних ресурсів, інформаційного середовища та інфраструктурної бази країни.

Водночас захист інформаційних ресурсів полягає в розробці та впровадженні методів, засобів і процедур кіберзахисту, які забезпечують стабільність функціонування інформаційних, телекомунікаційних і технічних систем. Даний механізм включає забезпечення технічної та організаційної безпеки всіх критичних елементів інфраструктури

Заключним завданням інформаційної безпеки в Україні є моніторинг та виявлення незвичайних подій у кіберпросторі та збір інформації, щоб своєчасно реагувати на потенційні загрози, що дозволяє своєчасно виявити аномалії та визначити їх причини.

3. Проаналізовано класифікацію цифрових інструментів кіберзахисту державних інформаційних ресурсів, в ході якого було визначено, що такі інструменти як Norton, Bitdefender і McAfee, захищають від шкідливого ПЗ, а інструменти для аналізу трафіку, наприклад Wireshark, допомагають виявляти загрози. Системи виявлення вторгнень, як Snort, контролюють мережеву активність, а інструменти для сканування вразливостей, такі як Nessus і Nmap, ідентифікують слабкі місця в інфраструктурі. Разом ці інструменти забезпечують комплексний захист від кібератак і підтримують безпеку даних.

Сучасні методи реалізації заходів кібербезпеки мають ґрунтуватися на стратегічних документах та державних програмах, які передбачають модернізацію систем захисту, розвиток адміністративно-правових процедур, удосконалення технічних аспектів.

Основними напрямками посилення захисту як держави, так і корпоративного сектору є оновлення правового законодавства з імплементацією міжнародних стандартів кіберзахисту та протидії кіберзлочинності, а також впровадження інновацій у засоби захисту цифрової інфраструктури.

Забезпечення національної стійкості проти кіберзагроз є критичним викликом, особливо в контексті триваючої російської агресії. Це вимагає

підвищеної уваги до розробки стратегій захисту національних інформаційних активів і підтримки їх цілісності та доступності в умовах зростання кіберзагроз.

4. Досліджено нормативно-правове регулювання кіберзахисту державних інформаційних ресурсів, що здійснюється як на міжнародному, так і на національному рівнях. Було проаналізовано чинні нормативно-правові акти (закони та постанови КМУ) і виявлено, що інформаційна безпека є невід'ємною частиною національної безпеки, що вимагає розробки ефективних механізмів захисту інформаційних ресурсів, систем їх формування, обробки та поширення, а також захисту інформаційної інфраструктури, конфіденційної, службової та персональної інформації.

Україна змогла досягти значних досягнень у сфері нормативно-правового регулювання інформаційної безпеки. Наявні функціональні характеристики системи зумовлені тим, що забезпечення інформаційної безпеки стало одним із головних пріоритетів державного управління.

Сучасне інформаційне середовище має значний вплив на політичну, економічну, військову та інші сфери національної безпеки України. Як свідчить аналіз чинного законодавства, інформаційна безпека є невід'ємною складовою національної безпеки, яка потребує ефективних механізмів захисту інформаційних ресурсів, систем їх формування, обробки та розповсюдження, а також необхідний розвиток інфраструктури захисту інформації.

5. Розглянуто значення системи національної безпеки в кіберекономічному просторі, що є сукупністю узгоджених елементів, кожен з яких виконує конкретні завдання в межах єдиного плану і стратегії. Ці елементи формуються та розгортаються в кіберпросторі для забезпечення безпеки інформаційних, телекомунікаційних та інформаційно-комунікаційних систем, забезпечення їх належного функціонування та захисту від кіберзагроз.

Багаторівневий підхід дозволяє створити ефективну та комплексну систему забезпечення інформаційної безпеки в Україні, де кожен рівень відповідає за виконання конкретних завдань та функцій. На перших трьох рівнях система національної безпеки забезпечується, контролюється та гарантується державними

органами, але на четвертому рівні це більше моральний імператив. Діяльність неурядового сектору є важливою частиною забезпечення двосторонньої комунікації та взаємодії громадських та державних інституцій. Однак ця сфера має унікальні вразливі місця, оскільки неурядові організації можуть бути привабливими мішенями для операцій іноземних спецслужб і слугувати ефективним інструментом для здійснення зовнішнього розвідувального впливу.

Одним із головних завдань системи інформаційної безпеки України є захист національних інтересів в інформаційному просторі. Загалом в Україні розроблено комплексну та багаторівневу систему управління інформаційною безпекою, яка ефективно відповідає на такі сучасні виклики, як кібератаки, інформаційні війни, шпигунство та зовнішнє втручання у внутрішні справи держави.

У цій системі основну роль виконує Державна служба спеціального зв'язку та захисту інформації, яка координує заходи, спрямовані на забезпечення криптографічного та технічного захисту інформаційних ресурсів. Діяльність служби не лише гарантує стабільність та надійність зв'язку між державними інституціями, а й забезпечує інтегрований захист інформаційних систем та забезпечує інформаційну безпеку на всіх рівнях державного управління та прийняття рішень.

6. Досліджено стан розвитку кібербезпеки України, в ході якого було визначено, що Україна постійно вдосконалює власний підхід до забезпечення державних інформаційних ресурсів, особливо в світлі впливу російської військової агресії. Водночас існує необхідність комплексного підходу до вдосконалення державної політики в сфері кіберзахисту, зокрема шляхом оновлення нормативно-правової бази, підвищення кваліфікації фахівців та розвитку відповідних інфраструктурних рішень.

Кібератаки становлять серйозну загрозу для багатьох секторів економіки, включаючи енергетику, промисловість, логістику, комунікації та програмне забезпечення. Однак найбільш небезпечні та руйнівні атаки за останній час були спрямовані на фінансовий сектор України, особливо на її великі банки. Такі атаки серйозно впливають на економічну стабільність країни, особливо на довіру до

фінансових установ і безпеку фінансових операцій, що, у свою чергу, створює ризик для економічного зростання та національної безпеки.

Відтак у 2023 році головними цілями кібератак стали державні та місцеві органи влади, служби безпеки та оборони, а системи виявлення та реагування на кіберуразливості (CRI) обробили приблизно 18 мільярдів подій, отриманих через системи моніторингу кібератак і телеметричних систем передачі даних.

Важливим аспектом зміцнення кібербезпеки України є міжнародна співпраця. Одним із важливих кроків у цьому напрямку є створення новітніх механізмів взаємодії країн Західної Європи, Канади та США у сфері кібербезпеки, зокрема наразі одним з таких активно функціонує «Талліннський механізм».

Ще одним важливим викликом у правових аспектах забезпечення кіберзахисту в Україні є використання штучного інтелекту (ШІ) у сфері кібербезпеки, особливо в контексті національного та міжнародного права.

7. Окреслено основні напрями забезпечення інформаційної безпеки держави відповідно до світового досвіду. Визначено, що досвід інших країн у забезпеченні інформаційної безпеки є важливим для України, особливо в контексті створення національного інформаційного простору. Це включає розвиток механізмів попередження загроз, наукове обґрунтування цих загроз, а також формування ефективної системи громадського інформаційного управління. Крім того, важливим аспектом є створення спеціалізованих інституцій, які забезпечуватимуть захист національних інтересів в інформаційній сфері.

8. Розроблено напрями вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації. Зокрема, в сучасних умовах, через вплив тривалої війни, забезпечення інформаційної безпеки є однією з головних пріоритетних завдань для України.

Серед основних викликів – це кіберзагрози, інформаційна війна, технологічні труднощі та психологічний вплив на громадян. Для ефективної протидії цим загрозам необхідно застосовувати комплексний підхід, який включає оновлення системи кіберзахисту, розробку стратегій боротьби з дезінформацією,

модернізацію технічної інфраструктури та підвищення стійкості населення до маніпуляцій.

9. Запропоновано перспективи розвитку кіберзахисту державних інформаційних ресурсів з використанням сучасних цифрових інструментів. Даний комплекс заходів передбачає інтеграцію сучасних цифрових технологій, таких як штучний інтелект, хмарні обчислення, біометричні системи та моделі Zero Trust. Вони дозволяють значно покращити рівень безпеки завдяки автоматизації процесів моніторингу, оперативному виявленню загроз та забезпеченню гнучкої ідентифікації доступу.

Використання цих інструментів дозволяє державним установам ефективно протистояти новим кіберзагрозам, знижуючи ризики витоку інформації та зловмисних атак. Водночас важливо забезпечити належний контроль і регулювання використання таких технологій, щоб мінімізувати потенційні ризики для національної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Східницька Г. Консолідація державних електронно-інформаційних ресурсів в Україні з використанням зарубіжного досвіду. *Вдосконалення обліку, фінансово-кредитного механізму в аграрному секторі та інформаційного*…2021. С.90-95.

2. Закон України «Про Національну програму інформатизації» від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 05.11.2024).

3. Постанова КМУ «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» від 12 березня 2022 року № 263. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF (дата звернення: 05.11.2024).

4. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» від 27.03.2014 № **1170-VII**. URL: https://zakon.rada.gov.ua/laws/show/1170-18#Text (дата звернення: 05.11.2024).

5. Блінова Г. Становлення України як цифрової держави та удосконалення системи державних електронних інформаційних ресурсів. *Law. State. Technology*. 2021. №2. С.3–10.

6. Закон України «Про Раду національної безпеки і оборони України» від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (дата звернення: 05.11.2024).

7. Блінова Г. О. Правові засади використання електронних інформаційних ресурсів в концепції цифрової держави. *Проблеми сукчасних трансформацій. Серія: право, публічне управління та адміністрування*. 2021. №2. С. 53-60.

8. Троян С.С. Інформаційно-безпекова політика Європейського Союзу. *Зовнішні справи.* 2019. № 2-3. С. 28–32.

9. Гайдук О., Звєрєв В. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. № *3*(23). С. 225–236.

10. Інформаційна безпека та кібербезпека держави: навчальний посібник [Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх , Р. О. Яворська]; за заг. ред. М. М. Присяжнкжа. Київ: Видавництво Ліра-К, 2024. 224 с.

11. Кулаковська І. Ризики використання хмарних технологій. *Herald of Khmelnytskyi National University. Technical Sciences*. 2024. № 341(5). С 45-52

12. Панченко О. А., Гнатенко В.С. Економічна кібербезпека в державній системі національної безпеки. *Публічне урядування*. 2021. №2 (27). С. 22-31.

13. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 223. № (3(63). С. 38-42.

14. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки України. *Підприємництво, господарство і право.* 2019. № 9. С. 100–108.

15. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ : КНТ, 2006. 280 с.

16. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2020. № (29). С. 281-288.

17. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник*. 2020. № 3. С. 18–26.

18. Подорожна Т. С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. *Аналітичне-порівняльне правознавство.* 2023. №6. С. 491-497.

19. Abrahams T., Ewuga S. A review of cybersecuritystrategies in modern organizations: examining theevolution and effectiveness of cybersecurity measures fordata protection. *Computer Science & IT Research Journal*, 2024. № 5. URL:

https://www.researchgate.net/publication/377346019_A-_review_of_cybersecurity_strategies_in_modern_org-aniz ations _examin ing_the _evolu tion_an d_effe cti-veness_of_cybersecurity_measures_for_data_protection (дата звернення: 28.10.2024).

20. Ukraine. National Cyber Security Index. URL: https://ncsi.ega.ee/country/ua/ (дата звернення: 20.10.2024).

21. Сайт Norton URL: https://www.norton.com (дата звернення:18.11.2024).

22. Сайт Bitdefender. URL: https://www.bitdefender.com (дата звернення:04.11.2024).

23. Сайт Mcafee URL: https://www.mcafee.com (дата звернення: 02.11.2024).

24. Сайт Tenable URL: https://www.tenable.com (дата звернення:05.11.2024).

25. Сайт Wireshark URL: https://www.wireshark.org/ (дата звернення:01.11.2024).

26. Сайт Snort URL: https://www.snort.org (дата звернення:03.11.2024).

27. Сайт Nmap URL: https://www.nmap.org (дата звернення:01.11.2024).

28. Корніленко О., Білик О. Аналіз відомих цифрових інструментів кібербезпеки. *За матеріалами конференції МНЛ* від 24 листопада 2023 р., м. Житомир. 2023. С.93–94.

29. Пугачов О. І. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. № (12). URL: https://reicst.com.ua/pmtl/article/view/2024-12-02-15/2024-12-02-15 (дата звернення: 01.11.2024).

30. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 20.10.2024).

31. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada. gov.ua/laws/show/2163-19 (дата звернення: 05.11.2024).

32. Закон України «Про оборону України» від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 05.11.2024).

33. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 05.11.2024).

34. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 05.11.2024).

35. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 05.11.2024).

36. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 05.11.2024).

37. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 05.11.2024).

38. Закон «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 5 липня 1994 року. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 05.11.2024).

39. Закон «Про електронні документи та електронний документообіг» № 851-IV від 22 травня 2003 року. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 05.11.2024).

40. Закон України «Про національну поліцію» 580-VIII від 16.08.2024 р.. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 05.11.2024).

41. Закон України «Про Службу безпеки України» від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 05.11.2024).

42. Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.19 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 05.11.2024).

43. Постанова КМУ «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних

ресурсів та інформації, вимога щодо захисту якої встановлена законом» від 11.11.2020 №1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (дата звернення: 05.11.2024).

44. Постанова КМУ «Деякі питання об’єктів критичної інформаційної інфраструктури» від 09.10.2020 №943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 05.11.2024).

45. Постанова КМУ «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» від 12.03.2022 № 263. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (дата звернення: 05.11.2024).

46. Постанова КМУ «Деякі питання подання інформації у сфері захисту критичної інфраструктури» від 14.10.2022 №1175. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-%D0%BF#Text (дата звернення: 05.11.2024).

47. Постанова КМУ «Деякі питання паспортизації об'єктів критичної інфраструктури» від 04.08.2023 № 818. URL: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#Text (дата звернення: 05.11.2024).

48. Постанова КМУ «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» від 28.04.2023 №415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (дата звернення: 05.11.2024).

49. Постанова КМУ «Про затвердження Положення про організаційно-технічну модель кіберзахисту» від 29.12.2021 №1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення: 05.11.2024).

50. Постанова КМУ «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» від 24.03.2023 №257. URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text (дата звернення: 05.11.2024).

51. Котляров В. Система забезпечення інформаційної безпеки України. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № (2(74). С. 45-49.

52. Столбовий В. М., Кисленко Д. П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджеталізації суспільства. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2023. №37.С. 175-183.

53. Ржевська Н. Ф. Сучасна інформаційна політика: досвід США для України. *Політична культура та ідеологія*. 2024. № 1 (7). С. 68-85.

54. Батько І., Павленко Д. Міжнародний досвід формування та становлення інституту інформаційної безпеки як невід'ємної складової сучасної держави. *Аналітично-порівняльне правознавство*. 2023. № 6. С.397-401.

55. Захаренко К.В. Міжнародний досвід інформаційної безпеки. *Сучасне суспільство*. 2019. №. 4. С. 95–109.

56. Ворохоб М., Киричок Р., Яскевич В., Добришин Ю., Сидоренко С. Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. № 1 (21). С. 223–233.

57. Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні. Науковий вісник Ужгородського Національного Університету. 2024. № 84. С. 77-83.

58. Бєлєвцева В. Основи правового регулювання інформаційної сфери у державі Ізраїль. Інформація і право. 2024. № 1(48). С. 162–169

59. Кузнєцов О.М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. *Інформація і право*. 2021. № 1(36). С. 106-113.

60. Петров С.Г. Проблеми захисту державних електронних інформаційних ресурсів у контексті цифрових трансформацій і цифровізації в Україні. *Порівняльно-аналітичне право*. 2020.№3.126-132.

61. Попов О.П. Безпекові аспекти цифрової взаємодіїу системі органів публічної влади в Україні. *Державне управління. Інвестиції: практиката досвід*.2024. №16. 309-314.

62. Красноступ Г.М. Правове регулювання забезпечення доступу до публічної інформації під час правового режиму воєнного стану в україні. *Інформація і право.* 2023. № 3 (46). С. 55-63.

63. Ткачук Н.В. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

64. Паршина О. А., Паршин Ю. І. Кібербезпека в сучасних умовах зростання загроз національній та світовій безпеці. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2024. № 1. С. 36–44.

65. Лопатченко І. С. Застосування досвіду США у використанні штучного інтелекту в забезпеченні національної інформаційної безпеки України. *Державне будівництво*. 2024. № 1 (35). С. 247–257.

66. Арсенович Л. А. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. Кібербезпека: освіта, наука, техніка. 2022. №3 (15). URL:https://csecurity.kubg.edu.ua/index.php/journal/article/download/338/281 (дата звернення: 25.10.2024).

67. Биков В. Ю., Романовський О. О., Романовська Ю. Ю. Навчання кібербезпеки і кіберзахисту фахівців з управління фінансами, економікою і бізнесом. ІТЗН. 2020. № 80 (6). С. 386–413.

68. Горбаченко С. Кібербезпека як складова економічної безпеки України. Galician economik journal. 2020. № 5 (66). С. 180–186.

69. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. Юридичний науковий журнал. 2023. № 1. С. 267-270.

70. Євсюкова О.В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. Державне управління: удосконалення та розвиток. URL:http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf (дата звернення: 20.10. 2024).

71. Звіт за результатами аналітичного дослідження «Стан та перспективи розвитку державних електронних інформаційних ресурсів». 48 с. URL: https://tapas.org.ua/wp-content/uploads/2020/08/1530105013.pdf (дата звернення: 01.01.2024).

72. Ігнатенко Р. В. Розвиток цифрового маркетингу у світі та в Україні. Бізнес Інформ. 2022. № 1. С. 450–455.

73. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 20.10.2024).

74. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. Innovation and Sustainability. 2022. № 3. С. 26–37.

75. Лахтадир С.Л. Кібербезпека як елемент інформаційної безпеки держави. Юридичний науковий електронний журнал. 2021. №4. С236-239.

76. Легомінова, С., Гайдур Г. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Кібербезпека: освіта, наука, техніка. 2023. № 2 (22). С. 54–67

77. Машталір В., Гук О., Мурасов Р., Фараон С., Лоза В. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 1 (49). С. 93-104.

78. Михальченко Г. Г., Снітко Ю. М., Іваненко В. О. Кібербезпека в економіці: захист від кіберзагроз у диджиталізованому світі. Наукові записки Львівського університету бізнесу та права. 2023. № 38. С. 377–383.

79. Олексюк Л. Правова база кібербезпеки в Україні: загальний огляд і аналіз. Міжнародна фундація виборчих систем. 2021. С. 7-57.

80. Омельченко А. В. Організаційно-правові засади забезпечення кібербезпеки України. Київський часопис права. 2021. № 3. С. 140-145.

81. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Економіка і регіон. 2022. № 1 (84). С. 13–20.

82. Петруха Н. М., Петруха С. В., Жмаєв А. Ю., Синкевич М. Е. Кібербезпека економіки та державних фінансів: історіографія та повоєнна траєкторія розвитку. Бізнесінформ. 2024. № 6. URL: https://www.business-inform.net/export_pdf/business-inform-2024-6_0-pages-64_79.pdf (дата звернення: 20.10.2024).

83. Постанова КМУ «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» від 14.10.2022 №1174. URL: https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text (дата звернення: 05.11.2024).

84. Потій О., Семенченко. А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту. Науковий вісник: Державне управління. 2021. № 3(9). С. 136-162.

85. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації. URL: https://www.kmu.gov.ua/ua/npas/pro-shvalennya-ukrayinina-2018-2020-roki (дата звернення: 16.10.2024).

86. Сайт Держспецзв'язку України. URL: https://cip.gov.ua/ua (дата звернення: 04.11.2024).

87. Сайт Lastpass URL: https://www.lastpass.com (дата звернення:05.11.2024).

88. Скіцько О., Ширшов Р. Нормативно-правове забезпечення кібероборони України: сучасний стан. Юридичний вісник. 2024. № 3. С. 244-250.

89. Стендер С. В, Фротер О. С., Снітко Ю.М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. Академічні візії. 2023. № 26. С. 1-13.

90. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. Адміністративне право і процес; фінансове право; інформаційне право. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2020. №2. С.119-124.

91. Цюцюра С. В., Київська К. І., Терентьєв О. О. Дослідження сфери кібербезпеки в Україні. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.). 2020. С.46-47.

92. Указ Президента України від 10.11.2019 р. № 837 «Про невідкладні заходи з проведення реформ та зміцнення держави». Офіційний вісник Президента України. 2019. № 24. Ст. 1038.

93. 2023 року кількість зареєстрованих кіберінцидентів зросла на 62,5%: звіт оперативного центру реагування на кіберінциденти ДЦКЗ. URL: https://www.inss.org.il/ https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz (дата звернення: 20.10.2024).

94. Cohen M.S., Freilich C.D., & Siboni G. Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 2015. 1–15. URL: https://www.inss.org.il/ he/wpcontent/ uploads/sites/2/systemfiles/Israel%20and%20cyberspace.pdf (дата звернення: 20.10.2024).

95. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent development. Energy Reports, 2021. № 7. P. 8176–8186.

96. Stancu A.I., Pavel T. Unveiling Israel’s Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies. Perspectives of Law and Public Administration. 2023. № 12(4). P. 643–650

97. World Economic Forum. Why we need global rulesto crack down on cybercrime. Jan 2, 2023. URL: https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/ (дата звернення: 28.10.2024).

ДОДАТКИ

Додаток А

Таблиця А.1 - Переліки та реєстри відкритих даних в частині охорони довкілля, доступ до яких може бути обмежено

Назва державного органу	Перелік даних
ДРС	Дані інтегрованої автоматизованої системи державного нагляду (контролю)
Мінекономрозвитку	Реєстр затверджених типів засобів вимірювальної техніки
	Державний реєстр наукових метрологічних центрів, метрологічних центрів і повірочних лабораторій, уповноважених на проведення повірки законодавчо регульованих засобів вимірювальної техніки, що перебувають в експлуатації
	Інформація про зареєстровані національні еталони
	Реєстр призначених органів з оцінки відповідності і визнаних незалежних організацій
	База даних про технічні регламенти
	Перелік проектів міжнародної технічної допомоги за підтримки країн-донорів, що реалізуються в Україні та пройшли державну реєстрацію (перереєстрацію) у Мінекономрозвитку
	Реєстр інвестиційних проектів і проектних (інвестиційних) пропозицій
Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості»	Український класифікатор нормативних документів
	Каталог національних стандартів і кодексів усталеної практики
	Національні стандарти, на які є посилання в нормативно-правових актах
	Національний банк стандартизованих науково-технічних термінів
МОЗ	Державний реєстр небезпечних факторів
	Державні санітарні норми та правила
	Гігієнічні нормативи
Міненерговугілля	Екологічна та радіаційна обстановка в зоні розташування атомних електростанцій
	Національний звіт у рамках Ініціативи прозорості видобувних галузей
Держенергоефективності	База даних енергетичних сертифікатів
	Реєстр альтернативних видів палива Державного агентства з енергоефективності та енергозбереження України
Міндовкілля	Реєстр екологічних аудиторів та юридичних осіб, що мають право на здійснення екологічного аудиту
	Перелік пестицидів і агрохімікатів, дозволених для використання
	Узагальнені дані регіональних реєстрів об’єктів утворення, оброблення та утилізації відходів України
	Державний кадастр тваринного світу
	Державний кадастр територій та об’єктів природно-заповідного фонду
	Дані про державні випробування та реєстрацію пестицидів і агрохімікатів
	Дані державної системи моніторингу довкілля
	Перелік міжнародних угод у сфері охорони навколишнього природного середовища, стороною яких є Україна, та стан їх виконання
	Дані про видані ліцензії на провадження господарської діяльності з поводження з небезпечними відходами та ліцензіатів

Назва державного органу	Перелік даних
	Дані про видані ліцензії на провадження господарської діяльності з виробництва особливо небезпечних хімічних речовин та ліцензіатів
	Єдиний реєстр з оцінки впливу на довкілля
	Державний реєстр суб'єктів господарювання, які здійснюють приймання та/або розбирання транспортних засобів, що утилізуються
	Перелік об'єктів, які є найбільшими забруднювачами навколишнього природного середовища по скиданню забруднюючих речовин у водні об'єкти
	Перелік висновків про транскордонне перевезення відходів
	Перелік дозволів на ввезення на митну територію України незареєстрованих пестицидів і агрохімікатів, що використовуються для проведення державних випробувань та наукових досліджень, обробленого ними насіннєвого (садивного) матеріалу, на використання залишків пестицидів і агрохімікатів, термін реєстрації яких закінчився
	Перелік дозволів на спеціальне використання об'єктів тваринного світу
	Розрахункові лісосіки
	Норми відстрілу інших мисливських тварин, віднесених до державного мисливського фонду, у сезон полювання
	Перелік дозволів на проведення робіт (крім будівельних на землях водного фонду)
	Перелік дозволів на імпорт та експорт видів дикої фауни і флори, сертифікатів на пересувні виставки, реекспорт та інтродукцію з моря зазначених зразків, за винятком осетрових риб і виробленої з них продукції
	Ліміти, норми використання об'єктів тваринного світу (крім водних біоресурсів) та спеціального використання об'єктів тваринного світу (крім водних біоресурсів)
	Ліміти на спеціальне використання природних ресурсів у межах територій та об'єктів природно-заповідного фонду загальнодержавного значення
	Державний класифікатор відходів
	Перелік дозволів на викиди забруднюючих речовин в атмосферне повітря стаціонарними джерелами об'єктів 1, 2, 3 груп із зазначенням номеру та строку дії
	Перелік декларацій про відходи, які подаються суб'єктами господарювання
	Перелік установ природно-заповідного фонду, що належать до сфери управління Мінприроди
	Перелік суб'єктів господарювання, яким Мінприроди затверджено показники емісії (питомі викиди) забруднюючих речовин в атмосферне повітря
	Перелік дозволів на добування тварин, внесених до Червоної книги України, та дозволів на збирання рослин, внесених до Червоної книги України
	Перелік дозволів на провадження діяльності, пов'язаної із штучними змінами стану атмосфери та атмосферних явищ у господарських цілях
	Перелік дозволів на транзитне переміщення не зареєстрованих в Україні генетично модифікованих організмів
	Перелік дозволів на проведення державної апробації (випробування) генетично модифікованих організмів у відкритій системі
	Червона книга України
	Зелена книга України
Держгеонадра	База даних спеціальних дозволів на користування надрами
	Інтерактивна карта ділянок надр, на які надано спеціальні дозволи користування надрами
	Об'єкти для залучення інвестицій
	Дані державного кадастру родовищ і проявів корисних копалин
	Дані державного кадастру родовищ підземних вод
	Дані реєстру нафтових і газових свердловин

Назва державного органу	Перелік даних
	Дані державного балансу запасів корисних копалин
	Інформація про стан мінерально-сировинної бази України
	Оглядові геологічні карти
	Державний водний кадастр за розділом «Підземні води»
	Дані про надходження заяв про надання, продовження, переоформлення та анулювання спеціальних дозволів на користування надрами, внесення змін до них та видачу їх дублікатів
	Реквізити та посилання на скановані копії документів, отримані та/або направлені Держгеонадрам під час виконання повноважень у сфері розгляду заяв про надання, продовження, переоформлення та анулювання спеціальних дозволів на користування надрами
	Дані про ділянки надр, щодо яких відбувається вирішення питання про організацію укладення угоди про розподіл продукції
	Дані про ділянки надр, щодо яких відбувається вирішення питання про продаж спеціального дозволу на користування надрами без проведення аукціону
	Дані про ділянки надр, щодо яких відбувається вирішення питання про продаж спеціального дозволу на користування надрами на аукціоні
	Каталог відомостей про геологічну інформацію з даними про її вартість
Держекоінспекція	Інформація про ефективність здійснення державного нагляду (контролю) територіальними органами Держекоінспекції
	Річний план здійснення заходів державного нагляду (контролю)
	Звіт про виконання річного плану здійснення заходів державного нагляду (контролю)
	Інформація про результати здійснення державного нагляду (контролю) у сфері охорони навколишнього природного середовища
Держводагентство	Дані державного моніторингу поверхневих вод
	Реєстр виданих дозволів на спеціальне водокористування
	Державний водний кадастр за розділами: “Водокористування” “Поверхневі води” у частині обліку поверхневих водних об’єктів
Держпродспоживслужба	Реєстр виробників органічної продукції (сировини)
	Реєстр висновків державної санітарно-епідеміологічної експертизи, виданих Держпродспоживслужбою
Мінрегіон	Перелік експертних організацій, що можуть проводити експертизу проектів будівництва
	Державні та галузеві будівельні норми
	Перелік базових організацій з науково-технічної діяльності у будівництві
	Перелік національних стандартів, які в разі добровільного їх застосування є доказом відповідності продукції вимогам технічного регламенту будівельних виробів, будівель і споруд
	Матеріали Генеральної схеми планування території України
Держгеокадастр	Державний реєстр сертифікованих інженерів-геодезистів
	Державний реєстр сертифікованих інженерів-землевпорядників
	Довідник показників нормативної грошової оцінки сільськогосподарських угідь в Україні
	Довідник показників нормативної грошової оцінки земель населених пунктів
	Державний реєстр оцінювачів з експертної грошової оцінки земельних ділянок
	Публічна кадастрова карта України
	Перелік матеріалів Державного картографо-геодезичного фонду
Держстат	Метаописи державних статистичних спостережень
	Результати статистичних спостережень (статистична інформація)

Назва державного органу	Перелік даних
Місцеві держадміністрації	Перелік дозволів на викиди забруднюючих речовин в атмосферне повітря стаціонарними джерелами об’єктів 2 та 3 груп із зазначенням номера та строку дії (для облдержадміністрацій)
	Схеми планування територій областей (для облдержадміністрацій)
	Схеми планування територій районів (для райдержадміністрацій)
Органи місцевого самоврядування	Основні положення генеральних планів населених пунктів та детальних планів територій
	Результати радіаційного контролю
	Генеральні плани населених пунктів, історико-архітектурні опорні плани, плани зонування територій та детальні плани територій (за винятком відомостей, які відповідно до законодавства становлять інформацію з обмеженим доступом), їх проекти
	Схеми планування територій та плани зонування територій (для сільських, селищних, міських рад)
	Дані про зелені насадження, що підлягають видаленню, відповідно до виданих актів обстеження зелених насаджень
	Дані про надані адміністративні послуги
	Дані містобудівного кадастру, у тому числі геопросторові дані

Джерело: [3]

Додаток Б

Таблиця Б.1 – Основні функції системи забезпечення інформаційної безпеки України

№	Функція	Завдання
1	Створення та забезпечення діяльності державних органів	- Розробка правових засад для системи.
		- Формування організаційної структури та раціональний розподіл функцій.
		- Забезпечення діяльності елементів системи (кадрове, фінансове, матеріальне, технічне, інформаційне забезпечення).
		- Підготовка елементів системи до функціонування.
2	Управління діяльністю системи	- Вироблення стратегії і планування заходів з інформаційної безпеки.
		- Організація і керівництво системою та її елементами.
		- Оцінка ефективності проведених заходів та витрат.
3	Планова та оперативна діяльність	- Визначення національних інтересів та їх пріоритетів в інформаційній сфері.
		- Прогнозування загроз і оцінка наслідків.
		- Запобігання і усунення впливу загроз на національні інтереси.
		- Локалізація і деескалація інформаційних конфліктів.
		- Ліквідація наслідків загроз.
4	Міжнародне співробітництво	- Розробка нормативно-правової бази для міжнародних інформаційних відносин.
		- Участь у двосторонніх і багатосторонніх міжнародних організаціях з інформаційної безпеки.
		- Спільне проведення заходів з іншими країнами та міжнародними організаціями.

Джерело: [5, 11, 15]

StrikePlagiarism.com

Дата звіту 11/21/2024
Дата редагування ---

Звіт не був оцінений.

Звіт подібності

метадані

Заголовок
Цифрові інструменти кіберзахисту державних інформаційних ресурсів

Автор
Пономаренко Ярослав Олександрович

Науковий керівник / Експерт
Осьмак А.С. д.філсоф.п.у.а

підрозділ
кафедра національної економіки та публічного управління

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		7
Білі знаки		0
Парафрази (SmartMarks)	a	91

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

КП 2

КЦ

25
Довжина фрази для коефіцієнта подібності 2

15862
Кількість слів

130543
Кількість символів

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)	
1	https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/sirovatchenko41.pdf	42	0.26 %
2	Cybersecurity in the context of modern threats: Israeli experience and its application in Ukraine В. Дзеньків;	30	0.19 %
3	Cybersecurity in the context of modern threats: Israeli experience and its application in Ukraine В. Дзеньків;	29	0.18 %
4	http://probudget.org.ua/news/yak-gromadam-realizuvati-pravo-na-dostup-do-publichnoyi-informatsiyi-v-umovah-voyennogo-stanu_944/	28	0.18 %

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені ВАДИМА ГЕТЬМАНА

Факультет економіки та управління

ЗБІРНИК ДОПОВІДЕЙ
91-ї щорічної студентської наукової конференції

«ІННОВАЦІЙНІ ПРОЄКТИ ДЛЯ ЕКОНОМІЧНОГО ВІДРОДЖЕННЯ ТА КОНКУРЕНТНОГО РОЗВИТКУ УКРАЇНИ»

15 квітня – 19 травня 2024 р.

КНЕУ КИЇВ 2024

УДК 657:336.221]:005.4(043)
І-66

Відповідальний за випуск:
к.е.н., доцент
кафедри бізнес-економіки та підприємництва Стариков О.Ю.

Рекомендовано до друку
Науково-експертною радою КНЕУ імені Вадима Гетьмана
Протокол № 6 від 20.06.2024 р.

І-66 **Інноваційні проєкти для економічного відродження та конкурентного розвитку України**: зб. доп. 91-ї щорічної студентської наукової конференції, 15 квітня – 19 травня 2024 р. [Електронний ресурс]. Київ, КНЕУ, 2024. 181 с.
ISBN 978-966-926-494-7

Збірник тез укладено за підсумками студентських досліджень, представлених на науковій конференції КНЕУ 15 квітня – 19 травня 2024 року. Доповіді здобувачів вищої освіти присвячено актуальним питанням розвитку бізнес-економіки та підприємництва, використанню кращих управлінських практик вітчизняними організаціями для відновлення і інноваційного розвитку економіки України. Розглянуто проблеми здійснення повоєнної інноваційної трансформації національної економіки, формування державної політики відродження України.

УДК 657:336.221]:005.4(043)

ISBN 978-966-926-494-7

КАФЕДРА МЕНЕДЖМЕНТУ

ПЛАТФОРМА
УПРАВЛІНСЬКІ ПРАКТИКИ ДЛЯ ВІДНОВЛЕННЯ
ТА ІННОВАЦІЙНОГО РОЗВИТКУ ЕКОНОМІКИ УКРАЇНИ

Пономаренко Я.О.
ОП «Державна політика та публічне управління», 1 курс магістратури
Київський національний економічний університет імені Вадима Гетьмана
Науковий керівник – д. філос. з публічного управління та адміністрування,
доцент кафедри національної економіки та публічного управління Осьмак А.С.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ КРИЗОВИХ ВИКЛИКІВ СЬОГОДЕННЯ

Проблема кіберзахисту державних інформаційних систем сьогодні займає провідне місце серед заходів підвищення ефективності діяльності публічного сектора. Актуальність вивчення даного питання обумовлена світовими тенденціями в розвитку інформаційно-технічного прогресу та як наслідок – появою нових загроз у цифровому середовищі, до яких можна віднести:

1) загальну тенденцію до зростання кількості кіберзлочинів через вдосконалення різноманітних технік викрадання даних та інструментів атак на роботу інфраструктури й державних систем;

2) постійний розвиток науково-технічного прогресу, зокрема поява штучного інтелекту, що спрощує можливості для здійснення кіберзлочинців, таким чином створюючи нові потенційні загрози для інформаційної безпеки;

3) пандемію COVID-19, що змусила багато компаній та установ переходити на дистанційну роботу, що призвело до збільшення кількості атак на цифрові ресурси через недостатній захист кіберпростору домашніх мереж та віддалених робочих середовищ;

4) збільшення кількості підключених пристроїв, що впливає на зростання потенційно вразливих точок входу для кіберзлочинців;

5) геополітичні конфлікти, оскільки держави використовують кібератаки як інструмент розвідки, впливу й навіть для ведення потенційних кібервійн, що підкреслює важливість кіберзахисту державних інформаційних ресурсів. Яскравим прикладом даного явища є протистояння України інформаційно-технічним операціям росії щодо дестабілізації роботи державних структур.

У цьому контексті кіберзахист державних інформаційних ресурсів стає критично важливим для забезпечення безпеки держави, її громадян та економіки в цілому.

XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Питома вага кіберзагроз стрімко зростає й дана тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття тільки посилюватиме свій вплив. Наявність таких загроз спонукає появі нових стратегій зі збереження безпеки у функціонуванні як національних, так і транснаціональних структур управління. Водночас між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення використати інструменти інформаційних технологій для реалізації власних геополітичних інтересів.

Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [1].

Для початку потрібно окреслити визначення системи державних електронних інформаційних ресурсів. Законодавець визначає дане поняття як «інформацію, яка є власністю держави та необхідність захисту якої визначено законодавством» [2].

Проте, дане визначення не дає повної картини відносно особливостей даної системи, тому створює умови для глибиннішого дослідження даного терміну. До прикладу А. Марущак

зазначає, що поняття «інформаційні ресурси держави» – це взаємозв'язана, упорядкована, систематизована, закріплена на матеріальних носіях інформація, яка створена, зібрана на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету. Інформаційні ресурси та інформаційний простір держави окреслено як основні об'єкти забезпечення інформаційної безпеки держави, що виступають основою інформаційного суверенітету України. При формуванні організаційно-правових основ захисту інформаційних ресурсів держави варто враховувати той факт, що до таких ресурсів нерідко включають і відомості, які належать недержавним суб'єктам: фізичним та юридичним особам [3].

Верховна Рада України 12 січня 2023 р. прийняла у першому читанні проєкт Закону про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури (реєстр. №8087). За наведеними у проєкті положеннями пропонується внести зміни до ряду законів України, спрямовані на нормативне забезпечення захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, на створення належної правової основи для здійснення заходів з попередження, виявлення і припинення актів агресії у кіберпросторі в умовах війни російської федерації проти України, а також на загальне удосконалення нормативно-правової бази у сфері кібербезпеки та захисту інформації задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам.

Зокрема, запропоновані зміни до законів України «Про Державну службу спеціального зв'язку та захисту інформації України» та «Про основні засади забезпечення кібербезпеки України» передбачають здійснення наступних заходів:

1) створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та визначення Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) уповноваженим органом, що здійснює забезпечення функціонування цієї системи;

2) покладання на Держспецзв'язку нових завдань щодо забезпечення кібербезпеки й кіберзахисту, державного контролю за додержанням вимог законодавства у сферах технічного захисту інформації та кіберзахисту тощо.

Серед інших пропозицій згідно зі Змінами до Закону України «Про основні засади забезпечення кібербезпеки України» пропонується:

1) створити в органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або 2 інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, підрозділи із кіберзахисту;

2) призначати у вищевказаних органах офіцерів із кіберзахисту, яким безпосередньо підпорядковуються підрозділи із кіберзахисту; надати право Держспецзв'язку визначати функції, повноваження, загальні вимоги до підрозділів із кіберзахисту та їх співробітників, а також особливості правового статусу та загальні вимоги до офіцерів із кіберзахисту.

Також законопроєктом передбачається виконання наступних особливих завдань:

1) визначити Міністерство закордонних справ України одним із основних суб'єктів національної системи кібербезпеки та закріпити його основні завдання у вказаній сфері;

2) встановити підвищений коефіцієнт нарахування посадового окладу співробітників підрозділів із кіберзахисту та офіцерів із кіберзахисту в органах державної влади та місцевого самоврядування;

3) закріпити Bug Bounty як одну зі складових порядку пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси та/або інформація, вимога щодо захисту якої встановлена законом, а також на об'єктах інформаційної критичної інфраструктури;

4) відокремити стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам тощо [4].

Для підвищення спроможності публічного сектору з розбудови кіберзахисту державних установ, Держспецзв'язку разом із проєктом ЄС «Підтримка комплексної реформи державно-

го управління в Україні» (EU4PAR) та Національним агентством України з питань державної служби (НАДС) провела перше навчання для держслужбовців категорії «А» з побудови кіберзахисту в державних установах. Курс був сертифікований Вищою школою публічного управління [5].

Отже, за останній час у сфері публічного управління було здійснено низку суттєвих кроків, що сприяють посиленню інформаційної безпеки держави. Водночас дана проблематика потребує більш детального дослідження, оскільки її значущість, враховуючи глобальні кризові перетворення, сьогодні є критично важливим вектором розвитку та збереження держави.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 №447/2021. URL : https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 12.05.2024).
2. Про затвердження Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління : Постанова Каб. Міністрів України від 03.08. 2005 р. № 668 URL : https://zakon.rada.gov.ua/laws/show/688-2005 (дата звернення: 11.05.2024).
3. Марущак А. Інформаційні ресурси держави : зміст та проблема захисту. *Правова інформатика.* 2009. № 1. С. 64-70. URL : http://nbuv.gov.ua/UJRN/Pinform_2009_1_12 (дата звернення: 12.05.2024).
4. Верховна Рада України прийняла законопроєкт щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. *Верховна Рада України.* URL : https://www.rada.gov.ua/news/razom/232072.html (дата звернення: 13.05.2024).
5. Підвищуємо кіберстійкість державних інформаційних ресурсів: Держспецзв'язку провела перший освітній курс із кіберзахисту для держслужбовців категорії «А». *Державний центр кіберзахисту Держспецзв'язку.* URL : https://scpc.gov.ua/uk/articles/225 (дата звернення: 13.05.2024).

Пушкарьова О.Д.
ОП «Цифрове врядування», 1 курс магістратури
Київський національний економічний університет імені Вадима Гетьмана
Науковий керівник – д. філос. з публічного управління та адміністрування,
доцент кафедри національної економіки та публічного управління Осьмак А.С.

ШЛЯХИ ВДОСКОНАЛЕННЯ ВЗАЄМОДІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ ТА ІТ-КОМПАНІЙ В УМОВАХ ЦИФРОВІЗАЦІЇ УКРАЇНИ

Цифровізація України є одним з ключових пріоритетів розвитку держави на сучасному етапі. Вона охоплює всі сфери життя суспільства, від надання державних послуг до розвитку економіки та освіти. Цифровізація має значний вплив на взаємодію органів публічної влади та ІТ-компаній. З одного боку, вона створює нові можливості для співпраці між ними. З іншого боку, вона також ставить перед ними нові виклики.

Для того, щоб максимізувати позитивний вплив діджиталізації на взаємодію органів публічної влади та ІТ-компаній, необхідно [1, с. 5]:

– створити сприятливе регуляторне середовище яке зможе стимулювати інновації та співпрацю між органами публічної влади та ІТ-компаніями;

– підвищити прозорість та підзвітність органів публічної влади перед громадськістю;

Наукове видання

ЗБІРНИК ДОПОВІДЕЙ
91-ї щорічної студентської наукової конференції

«ІННОВАЦІЙНІ ПРОЄКТИ
ДЛЯ ЕКОНОМІЧНОГО ВІДРОДЖЕННЯ
ТА КОНКУРЕНТНОГО РОЗВИТКУ УКРАЇНИ»

15 квітня – 19 травня 2024 р.

Видано в авторській редакції

Коректор *В. Македон*
Верстка *М. Криворученко*

Підп. до друку 03.07.2024. Формат 60×84/8.
Друк. арк. 7,54. Зам. 24-5850

Київський національний економічний університет імені Вадима Гетьмана
03680, м. Київ, проспект Берестейський, 54/1

Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи (серія ДК, № 235 від 07.11.2000)

E-mail: litera@kneu.edu.ua