ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Навчально-науковий інститут управління, економіки та бізнесу
Кафедра публічного адміністрування

«Допущено до захисту»
Завідувач кафедри
_____
І.А.Семенець-Орлова
«____»_____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського) рівня вищої освіти

на тему:

«ПУБЛІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ ДОСВІДУ ЗАХІДНИХ ПАРТНЕРІВ»

Виконав: студент групи
Е-8-23-М1ПУА(2.0з)
спеціальності 281 «Публічне управління та адміністрування»
Холкін Олег Анатолійович
Керівник: к.держ.упр., Телендій А.А.

Київ 2025

АНОТАЦІЯ

Холкін Олег Анатолійович. «Публічне управління інформаційною безпекою на основі досвіду західних партнерів».

Кваліфікаційна робота на здобуття рівня вищої освіти «магістр» із спеціальності «Публічне управління та адміністрування» - Міжрегіональна Академія управління персоналом – Київ. 2025

У кваліфікаційній роботі визначено теоретичні принципи публічного управління інформаційною безпекою. Проаналізовано організації забезпечення інформаційної безпеки в країнах Європейського союзу та США. Визначено шляхи удосконалення управління забезпеченням інформаційної безпеки.

Ключові слова: публічне управління, інформаційна безпека, державні органи, системи захисту, кібербезпека, інформаційний простір, громадянське суспільство.

SUMMARY

Kholkin Oleh. "Public Information Security Management Based on the Experience of Western Partners".

Thesis for obtaining the level of higher education "Master" in "Public Administration" - Interregional Academy of Personnel Management - Kyiv. 2025

The thesis defines the theoretical principles of public information security management. The organization of information security in the countries of the European Union and the United States is analyzed. Ways to improve information security management are identified.

Key words: public administration, information security, government agencies, security systems, cybersecurity, information space, civil society.

ЗМІСТ

ВСТУП 4

РОЗДІЛ 1 ТЕОРЕТИЧНІ ПРИНЦИПИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ 7

1.1 Поняття, сутність та історія виникнення проблеми забезпечення інформаційної безпеки 7

1.2 Принципи управління інформаційною безпекою 16

РОЗДІЛ 2 АНАЛІЗ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА США 24

2.1 Нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині 24

2.2. Характеристики інформаційної безпеки в державних органах (досвід США) 31

РОЗДІЛ 3 УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ 38

3.1 Адаптація досвіду країн ЄС з інформаційної безпеки 38

3.2 Методичні рекомендації щодо підвищення інформаційної безпеки та організації доступу до публічної інформації 51

ВИСНОВКИ 58

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 64

ВСТУП

Останнім часом питання національної безпеки стало не лише декларативним, а й практичним питанням. Значною мірою це зумовлено зростанням зовнішніх загроз стабільному розвитку України, зокрема посиленням мілітаризації сусідніх держав, використанням залежності нашої держави в енергетичній, торговельно-економічній сферах, зростанням економічного та інформаційного тиску та іншими викликами.

Враховуючи зростання значення інформації як ресурсу суспільного розвитку, а також вплив глобальних процесів на держави та нації, актуальним стає питання збереження та постійного оновлення національного інформаційного простору. В умовах інформаційної агресії він виступає не лише як основний об'єкт атаки, а й як ключовий елемент захисту для атакованої сторони.

Сучасний національний інформаційний простір як система обміну даними має включати розгалужену мережу структур, відповідальних за створення нової інформації, її захист і зберігання, а також організацію доступу до неї через засоби розповсюдження всередині країни та за кордоном. Головне завдання – задоволення інформаційних потреб громадян та забезпечення безпеки державної інформації.

Питання інформаційної безпеки в Європейському Союзі розглядається в контексті проблем розвитку інформаційного суспільства. Аналіз нормативно-правових актів та стратегічних планів ЄС у цій сфері свідчить про значно звужене трактування поняття «інформаційна безпека» порівняно з підходами, які застосовуються в Україні та міжнародному праві.

Реформування системи державного управління у сфері інформаційної безпеки передбачає адаптацію національної моделі до передового досвіду країн Європейського Союзу. У зв'язку з цим науково-практичним завданням є узагальнення досвіду забезпечення інформаційної безпеки в розвинених країнах світу, зокрема в ЄС та США.

Дослідження в цій галузі проводили вітчизняні та зарубіжні вчені, серед яких: Олександр Баранов, Олег Бондаренко, Михайло Кельман, Олександр Климчук, Віталій Коваль, Валерій Колпаков, Борис Кормич, Олексій Логунов, Василь Маклаков, Рена Марутян, Георгій Почепцов, Олександр Стрілець, Лідія Туманова, Петро Уфімцев, Володимир Шеломенцев.

Метою магістерської роботи є аналіз державного управління у сфері інформаційної безпеки в країнах Європейського Союзу та Сполучених Штатів Америки, а також використання його досвіду для підвищення рівня інформаційної безпеки в Україні.

були визначені наступні **завдання**:

- розглянути поняття, сутність та історичні аспекти проблеми інформаційної безпеки;
- охарактеризувати основні принципи її забезпечення;
- Дослідити нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині;
- проаналізувати функціонування системи захисту інформації в органах державної влади США;
- Визначити шляхи підвищення інформаційної безпеки в Україні шляхом адаптації передового міжнародного досвіду та вдосконалення організації доступу до публічної інформації.

Об’єктом дослідження є суспільні відносини, які формуються в процесі державного управління інформаційною безпекою в країнах Європейського Союзу та США.

Об’єктом дослідження є досвід державного управління у сфері забезпечення інформаційної безпеки в різних країнах ЄС та США.

Практичне значення роботи полягає в можливості застосування її результатів у наукових дослідженнях, у законотворчій діяльності, у навчальному процесі, а також у сфері правової освіти.

Наукова новизна дослідження полягає в теоретичному обґрунтуванні та практичному вирішенні комплексу питань управління у сфері інформаційної безпеки в Україні з урахуванням досвіду країн ЄС та США.

У процесі написання роботи було застосовано низку загальнонаукових

методів, зокрема метод аналізу наукових джерел, порівняльний аналіз, а також поєднання історичного та логічного підходів, міждисциплінарний метод з використанням розробок у галузі історії, політології та права.

Інформаційну базу дослідження складають нормативно-правові акти, статистичні та спеціальні періодичні видання, вітчизняні та зарубіжні наукові праці з предмета дослідження.

Структурно магістерська робота включає вступ, три розділи, висновки та список використаних джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ПРИНЦИПИ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Поняття, сутність та історія виникнення проблеми забезпечення інформаційної безпеки

Характеризуючи поняття, сутність та історію проблеми забезпечення інформаційної безпеки, слід зазначити, що в Радянському Союзі питання інформаційної безпеки та захисту інформаційного простору були покладені на створену в 1973 р. Державну комісію СРСР з протидії зовнішньотехнічній розвідці. За період її діяльності була побудована потужна система органів, відповідальних за захист інформації та забезпечення інформаційної безпеки.

8 грудня 1991 р. було підписано Угоду про створення СНД. 21 грудня того ж року глави одинадцяти незалежних держав, що раніше входили до складу СРСР, підписали Протокол про створення Співдружності та прийняли Алма-Атинську декларацію. Грузія приєдналася до СНД у 1993 році, але вийшла з Співдружності у 2010 році після російсько-грузинської війни 2008 року. 22 січня 1993 року Рада глав держав прийняла Статут СНД, який залишається чинним і сьогодні. Україна має статус держави-засновниці СНД, але ніколи не підписувала Статут.

Відповідно до положень Угоди та Статуту головною метою СНД є розвиток рівноправного та взаємовигідного співробітництва в різних сферах, зокрема сприяння вільному обміну інформацією та виконанню взаємних зобов'язань. Лише 18 жовтня 1996 року, майже через п'ять років після утворення Співдружності, була прийнята Концепція формування інформаційного простору СНД. Документ визначає завдання щодо забезпечення кожною державою-учасницею інформаційної безпеки та захисту інформаційного суверенітету. З цією метою країни взяли на себе зобов’язання відстежувати інформаційні загрози та вдосконалювати інформаційну

політику.

Водночас у тодішній редакції Концепції не були відображені питання, пов’язані з підготовкою та проведенням інформаційних воєн чи інформаційно-психологічних операцій. Це призвело до того, що один із ключових аспектів інформаційної безпеки тривалий час залишався поза межами правового регулювання.

Рішенням Ради глав урядів СНД від 25 листопада 1998 р. прийнято Перспективний план розробки документів і заходів щодо реалізації Концепції формування інформаційного простору СНД. У 1999 році Концепція інформаційної безпеки держав-учасниць СНД у військовій сфері була схвалена та підписана країнами-членами ОДКБ Вірменією, Білоруссю, Казахстаном, Киргизстаном, Російською Федерацією і Таджикистаном.

Відповідно до цієї Концепції основними джерелами загроз інформаційній безпеці у військовій сфері є: державна політика іноземних держав, спрямована на моніторинг політичних, економічних, військових, екологічних та інших процесів з метою отримання односторонніх переваг, а також відсутність єдиної політики, розвиненої інфраструктури та необхідної нормативно-правової бази у сфері інформаційної безпеки.

10 жовтня 2008 року в Бішкеку Рада глав держав СНД схвалила Концепцію співробітництва держав-учасниць СНД у сфері забезпечення інформаційної безпеки. Однак ці документи підписали лише країни-члени ОДКБ.

Іншими документами у сфері інформаційної безпеки СНД стали прийнята 28 вересня 2012 року Стратегія співробітництва держав-учасниць щодо розвитку інформаційного суспільства та План заходів щодо її реалізації до 2015 року, а також Модельний інформаційний кодекс держав-учасниць СНД. Ці документи підготовлені профільною організацією СНД з методичного, організаційного та технічного забезпечення роботи у сфері інформаційної безпеки та підготовки фахівців. 30 травня 2012 року рішенням Ради глав урядів СНД федеральному державному унітарному підприємству

надано статус базової організації.

В Україні 23 квітня 2008 року Рада національної безпеки і оборони (РНБО) ухвалила рішення №377/2008, згідно з яким Кабінету Міністрів доручено затвердити Доктрину інформаційної безпеки України, Державну програму формування позитивного іміджу України та перелік заходів щодо розширення фінансової підтримки культурно-інформаційних центрів у дипломатичних установах. Це рішення було скасовано 28 квітня 2014 року. Доктрина інформаційної безпеки України затверджена Указом Президента України № 514/2009, але втратила чинність Указом Президента України від 6 червня 2014 року № 504/2014.

Щодо сутності поняття «інформаційна безпека», то слід зазначити, що під цим терміном розуміють стан, за якого людина має можливість уникнути цілеспрямованого чи неусвідомленого негативного впливу інформації.

Таблиця 1.1. Характеристика поняття «інформаційна безпека» на думку різних вчених

Автор	**Характеристика поняття**
Р. А. Балта	«Інформаційна безпека – вид правовідносин публічної інформації щодо створення, підтримки та захисту безпечних умов життєдіяльності, бажаних для людини, суспільства і держави; публічно-правові відносини, пов'язані зі створенням, розповсюдженням, зберіганням і використанням інформації».
БАКАЛАВР МИСТЕЦТВ. Кермо	«Інформаційна безпека – стан захищеності встановлених законом норм і параметрів інформаційних процесів і відносин, що забезпечують необхідні умови для існування держави, людини і суспільства як суб’єктів цих процесів і відносин».
О. Л. Морозова	«Кібербезпека держави – стан державних інституцій і суспільства, що забезпечує надійний захист національних інтересів країни та її громадян в інформаційній сфері».
ВІРДЖІНІЯ. Ліпітос	«Інформаційна безпека – складова національної безпеки, процес управління загрозами і небезпеками з боку державних і недержавних інституцій та окремих громадян, забезпечення інформаційного суверенітету України».

Н. Р. Нижній, Г. П. Ситник, В. О. Білобородий	«Поняття інформаційної безпеки визначено виходячи з найбільш ймовірних загроз національній безпеці України у життєво важливих сферах. Зокрема, у сфері інформаційної безпеки науковці розуміють стан правових норм та пов'язаних з ними інститутів безпеки, які забезпечують постійну доступність даних для прийняття стратегічних рішень та захисту інформаційних ресурсів країни».

Проте варто детальніше розглянути, наскільки наведене визначення відповідає своїй суті та співвідноситься з поняттям «інформаційний простір». Щоб зрозуміти напрямок розвитку інформаційного простору, варто звернутися до поняття «кібернетика», похідною від якого є сучасна інформатика. Кібернетика визначається як «наука про управління, комунікацію та обробку інформації». Основним об'єктом дослідження в ньому є так звані кібернетичні системи, які аналізуються абстрактно, незалежно від їх матеріальної природи. Приклади кібернетичних систем включають автоматичні регулятори в технології, комп'ютерних системах, людському мозку, біологічних популяціях і соціальних процесах. Кожна з цих систем складається з взаємопов'язаних елементів, здатних отримувати, зберігати, обробляти та передавати інформацію, а також змінювати її.

Виходячи з вищесказаного, можна зробити висновок, що інформаційний простір – це форма існування сукупності матеріальних і нематеріальних об'єктів і процесів, які беруть участь у формуванні, сприйнятті, запам'ятовуванні, обробці та обміні інформацією.

Основними властивостями інформаційного простору є:

- «довжина»;
- «єдність судження і безперервність»;
- «матеріальність і нематеріальність»;
- «абстракція і реальність»;
- «реальність загального впливу».



Рисунок 1.1 Властивості інформаційного простору

Примітка: Підготовлено автором за джерелом [28]

Інформаційний простір має певний обсяг, який визначається кількістю матеріальних і нематеріальних об'єктів, доступних у певний період часу. У той час як кіберпростір обмежений фізичними межами Землі, інформаційний простір є практично необмеженим через наявність нематеріальних компонентів.

Інформаційний простір включає матеріальні елементи: техніку, засоби зв'язку, телекомунікаційні мережі, алгоритми та коди. Крім того, він включає нематеріальні компоненти: інформацію, процеси її сприйняття, зберігання, передачі та обробки. Варто зазначити, що в цьому контексті матеріальність розглядається не у філософському сенсі, а як усе, що може бути безпосередньо сприйняте чуттями.

Таким чином, інформаційний простір – це створене людиною середовище, яке виникло для задоволення його потреб, без урахування побічних ефектів, про які йтиметься далі.

На підставі вищесказаного можна зробити такі висновки:

Об’єктами інформаційного простору є живі істоти, їх групи та організації, здатні сприймати, переробляти, запам’ятовувати та перетворювати інформацію, зокрема індивіди, соціальні спільноти, держава, а також матеріальні та нематеріальні елементи, пов’язані з інформаційними процесами.

Суб'єктами кіберпростору є люди, суспільство, державні структури та інші живі організми, які можуть взаємодіяти з інформацією та змінювати її.

Проте більш глибокий аналіз поняття «інформаційна безпека» дозволяє виявити різницю між термінами «інформаційний простір» і «кіберпростір».

Інформаційний простір визначається як «форма співіснування сукупності матеріальних і нематеріальних об’єктів і процесів, призначених для задоволення інформаційних потреб усіх живих істот на Землі».

Відповідно до цього визначення, інформаційна безпека розглядається як «стан систем, який дозволяє нейтралізувати загрози доступності, цілісності та конфіденційності даних, що циркулюють в інформаційних системах». Крім того, оскільки IT-сервіси також є потенційно вразливими об’єктами, поняття інформаційної безпеки включає також ризики порушення роботи інформаційних систем вищого рівня.

Відповідно до німецької стратегії, «інформаційна безпека передбачає комплекс необхідних заходів, що мінімізують ризики». Основний акцент робиться на комплексному підході, який дозволяє розробити ефективні заходи захисту, хоча він не забезпечує достатньої методологічної бази для оцінки ефективності таких систем.

У Канаді інформаційний простір вважається стратегічним ресурсом, тому для його ефективного використання необхідно прогнозувати кіберзагрози та вживати заходів щодо їх нейтралізації. Водночас канадська стратегія не містить чіткого визначення поняття «інформаційна безпека», хоча детально описує види кіберзагроз та заходів протидії.

У Туреччині інформаційна безпека визначається як «захист

інформаційних систем в інформаційному просторі від атак, забезпечення конфіденційності, цілісності та доступності інформації, а також виявлення та реагування на кіберінциденти».

У Нідерландах Національна стратегія інформаційної безпеки, прийнята в 2013 році, визначає її як набір заходів для запобігання збоям у роботі ІКТ та неправильного використання, а також для відновлення систем після атак.

Австралійська стратегія інформаційної безпеки спрямована на «підтримку безпечного, стійкого та надійного електронного середовища, яке підтримує національну безпеку та розвиток цифрової економіки». У документі 2009 року наголошується на необхідності забезпечення конфіденційності, доступності та цілісності інформації, а також захисту громадян від кіберзагроз.

В Україні визначення інформаційної безпеки в законопроектах охоплює «стан захищеності життєво важливих інтересів людини, суспільства і держави в кіберпросторі». Однак такий підхід має низьку методологічну ефективність, оскільки розглядає кіберпростір лише як середовище функціонування інформаційно-телекомунікаційних систем, без урахування більш широкого кола загроз і проблем.

Оскільки питання інформаційної безпеки має глобальне значення, особливий інтерес викликає позиція міжнародних організацій. Зокрема, у Рекомендаціях Міжнародного союзу електрозв'язку зазначено, що інформаційна безпека – це «набір інструментів, стратегій, принципів безпеки, механізмів захисту, настанов, методів управління ризиками, освітніх заходів, практичних підходів, страхування та технологій, які можуть бути використані для захисту інформаційного середовища, організаційних ресурсів і користувачів» [28].

Інформаційні ресурси організацій і користувачів включають «підключені обчислювальні пристрої, персонал, комунікаційну інфраструктуру, програмне забезпечення, телекомунікаційні послуги та всі дані, що передаються або зберігаються в інформаційному просторі». Основною метою інформаційної безпеки є «забезпечення стійкості та захисту

ресурсів організації та користувачів від потенційних загроз». До основних принципів інформаційної безпеки належать конфіденційність, цілісність, достовірність, доступність і достовірність інформації [22, с. 24].

Проблема управління інформацією є невід'ємною складовою національної безпеки, оскільки ефективний контроль над інформаційними ресурсами безпосередньо впливає на стабільність держави. Виходячи з цього, інформаційну безпеку можна визначити як «стан суспільства, державний і людський потенціал, який забезпечує захист від цілеспрямованих або неусвідомлених інформаційних загроз». Інформаційна безпека передбачає захист від таких факторів:

- Поширення деструктивної інформації, яка може мати маніпулятивний або небезпечний характер;
- Несанкціонований доступ до інформаційних ресурсів та використання їх у шахрайських цілях;
- Вплив негативних інформаційних технологій, які можуть становити загрозу національній безпеці [42].

В умовах глобалізації інформація стає одним із найцінніших ресурсів. Рівень економічної конкурентоспроможності держав і підприємств значною мірою визначається рівнем розвитку інформаційної інфраструктури. Водночас сучасне інформаційне суспільство стикається з низкою загроз: зростання інформаційних маніпуляцій, кіберзлочинності, промислового шпигунства та витоку конфіденційних даних. Конституція України визначає інформаційну безпеку як одну з ключових функцій держави [4].

Наукові дослідження показують, що «сучасна система захисту інформації в Україні не виконує певних критичних функцій». Зокрема, спостерігається неефективний менеджмент та хаотичні організаційні реформи у сфері кібербезпеки. Негативні тенденції у національному інформаційному просторі, економічна криза, нестабільна політична ситуація та зовнішні загрози породжують ризики, які можуть завдати серйозної шкоди державним установам, громадянам та бізнесу [8, с. 90].

З огляду на це особливої уваги потребує координація дій державних органів, приватного сектору, громадських організацій та громадян. Відповідно до статті 17 Конституції України забезпечення інформаційної безпеки є «спільною справою всього Українського народу». Це актуальне питання, оскільки сфера інформаційних технологій розвивається дуже динамічно, що вимагає постійного оновлення методів захисту даних і боротьби з новітніми загрозами. Слід зазначити, що в сучасному цифровому середовищі зміни у сфері інформаційної безпеки часто є наслідком маркетингових стратегій великих корпорацій, які активно просувають власні технології [1].

Впровадження ефективної системи захисту інформації неможливе без впровадження нових концепцій, сучасних технологій та науково обґрунтованої політики. Важливими є пропозиції щодо активного залучення вітчизняних вчених і компаній до розробки власних інформаційних технологій. Це й створення якісного програмного забезпечення, розробка стандартів інформаційної безпеки, сертифікація обладнання та впровадження національних баз даних і телекомунікаційних систем [2].

Ігнорування цих питань може перешкодити прийняттю ключових політичних, економічних, військових і соціальних рішень. Від рівня інформаційної безпеки безпосередньо залежить політична стабільність, обороноздатність і стійкість національної економіки. Багато сучасних кіберзагроз спрямовані на підрив основних соціальних структур, створення хаосу та маніпулювання громадською думкою. Як зазначають експерти, «реалізація інформаційних загроз має руйнівні наслідки для політичної, економічної, військової та соціальної сфер» [18, с. 129].

Сьогодні в Україні відсутні реальні гарантії інформаційної безпеки, що зумовлено відсутністю чіткої нормативно-правової бази та недостатньою координацією між державними органами. Процес цифровізації відбувається хаотично, з надмірною залежністю від іноземних технологічних рішень, що підвищує вразливість інформаційного середовища.

Підсумовуючи вищесказане, слід зазначити, що дослідження проблеми

інформаційної безпеки в Україні та інших пострадянських країнах активно розпочалося лише в останнє десятиліття XX ст. Це було зумовлено процесами демократичних реформ та здобуттям незалежності. Інформаційна безпека визначається як «стан захищеності критично важливих інтересів людини, суспільства і держави в умовах функціонування інформаційних систем і телекомунікаційних мереж». Основні загрози включають:

- Неповнота, неточність або застарілість інформації, яка використовується при прийнятті рішень;
- Несанкціоноване втручання в потоки інформації, порушення її конфіденційності, цілісності та доступності;
- Негативний вплив деструктивної інформації на суспільні процеси та державні інститути.

Тому питання інформаційної безпеки стає критичним для національної безпеки України. Враховуючи глобальний характер загроз, необхідно розробити ефективні механізми захисту, адаптовані до сучасних викликів інформаційної доби.

1.2 Принципи управління інформаційною безпекою

Аналіз принципів інформаційної безпеки свідчить про те, що «в національному законодавстві вже закладені необхідні теоретичні основи для формування узагальненої системи принципів організації та управління інформаційною безпекою». Водночас із розвитком інформаційних технологій та цифрових загроз виникає потреба не лише уточнювати існуючі принципи, а й розробляти нові підходи, які зможуть ефективно відповідати на виклики сучасного інформаційного середовища.

Забезпечення інформаційної безпеки є складним і багаторівневим процесом, який потребує системного підходу та інтеграції різноманітних механізмів правового, організаційного, технічного та економічного характеру.

В умовах глобалізації та зростання ризиків, пов’язаних з кібератаками,

маніпулюванням інформацією, витоком даних та загрозами критичній інфраструктурі, питання вдосконалення принципів управління інформаційною безпекою стає особливо актуальним.

Одним із ключових питань сьогодення є необхідність чіткого методологічного обґрунтування засад, які визначатимуть ефективність державної політики щодо захисту інформації. Зокрема, важливо виділити наступні основні напрямки:

Оновлення нормативно-правової бази відповідно до сучасних світових стандартів інформаційної безпеки, зокрема шляхом гармонізації законодавства України з європейськими та міжнародними стандартами.

Розробити комплексну стратегію управління інформаційною безпекою, яка включає правові, організаційні, технологічні та соціальні аспекти.

Впровадження нових підходів до захисту інформації, що передбачають активне використання сучасних криптографічних методів, штучного інтелекту для аналізу загроз, а також кібергігієни користувачів інформаційних систем.

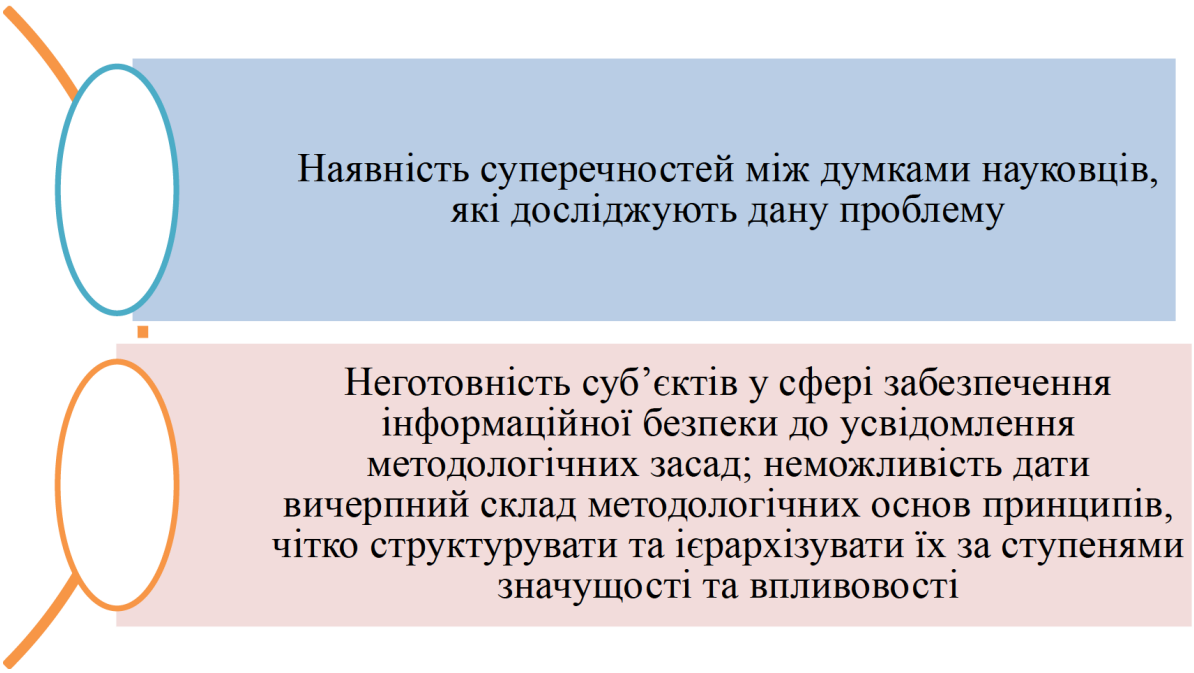
Підвищити рівень координації між державними органами, приватним сектором та громадянським суспільством з питань інформаційної безпеки.

Слід зазначити, що в сучасних умовах загрози інформаційній безпеці не обмежуються кіберзлочинністю. Це також інформаційно-психологічні операції, маніпулювання громадською думкою через цифрові платформи та вплив на виборчі процеси та економічні механізми шляхом інформаційних атак. Це потребує розширення підходів до забезпечення інформаційної безпеки, зокрема шляхом удосконалення методів виявлення та протидії загрозам інформації.

Також важливими є питання підготовки фахівців у сфері інформаційної безпеки та розширення міждисциплінарних досліджень, що поєднують правові, технічні, соціологічні та психологічні аспекти захисту інформації.

Тому складність проблеми методологічного обґрунтування принципів управління інформаційною безпекою потребує детального аналізу та розробки ефективної концепції, що враховує як сучасні виклики, так і

перспективи розвитку інформаційних технологій і космосу.



Малюнок 1.2. Основні причини проблеми визначення методологічних засад управління інформаційною безпекою

Примітка: підготовлено автором за джерелом [12, с. 76]

Як відомо, будь-який принцип управління як суспільне явище має чітко визначену мету та відповідний зміст. Загальною рисою всіх принципів управління є їх здатність визначати тенденції у формуванні певних характеристик об'єкта незалежно від конкретних умов. «Тому управління інформаційною безпекою на основі певних принципів передбачає виявлення наявних і потенційних можливостей, які забезпечують реалізацію відповідних характеристик об'єкта в часі та просторі» [12, с. 77].

Заснування конкретної системи принципів управління інформаційною безпекою сприяє підвищенню методичного рівня її організаційної адаптації до соціально-економічної ситуації в державі. Базуючись на чітких методологічних засадах, інформаційна безпека набуває системного характеру, забезпечуючи стабільність і дієвість механізмів її гарантування.

За своєю природою принципи права поділяються на соціально-економічні, політичні, ідеологічні, релігійні, естетичні та спеціально-правові.

Останні мають важливу характеристику: вони визначають, як право відображає соціальну основу суспільства, яка структура права і який характер правового регулювання суспільних відносин.

Відомий дослідник В. Колпаков, аналізуючи принципи державного управління, зазначає, що «принципи державного управління – це його позитивні закономірності, відомі науці і практиці та закріплені у відповідних концепціях» [14, с. [312]. Він включає такі ключові характеристики принципу управління:

- приналежність до відомих позитивних закономірностей, що характеризують стабільність та ефективність процесів управління;
- вкорінені в суспільній свідомості, реалізуються за допомогою правових механізмів, як правило, у формі правових норм.

Тому принципи управління інформаційною безпекою є невід'ємною частиною загальної системи державного управління та мають відповідати фундаментальним закономірностям правового регулювання. Вони забезпечують стратегічне спрямування державної політики у сфері захисту інформаційного простору, визначають ключові підходи до її регулювання та сприяють адаптації до сучасних викликів цифрової епохи.

Таблиця 1.2. Принципи державного управління

Ім'я	**Інгредієнти**
"Суспільно-політичний"	«демократизм, участь населення в управлінні державою; рівноправність людей різних національностей; рівність усіх перед законом; законність; прозорість та врахування громадської думки; об'єктивність»
«Організаційні засади побудови апарату державного управління»	«галузевий, функціональний, територіальний»

«Організаційні засади функціонування апарату державного управління»	«регламент діяльності, єдиноначальність, колегіальність, розподіл управлінської праці; відповідальність за прийняті рішення; оперативний незалежність»

Примітка: підготовлено автором за джерелом [14, с. 313].

Б. Кормич пропонує визначати принципи забезпечення інформаційної безпеки через два комплекси взаємопов’язаних питань, що відрізняються за характером правових норм, що утворюють їх нормативну базу. Перший комплекс стосується інформаційної безпеки особистості та суспільства, що пов’язано насамперед із свободою від державного втручання та реалізацією прав на самовизначення та самореалізацію. Другий комплекс охоплює державну інформаційну безпеку, яка, навпаки, базується на механізмах правового регулювання, зокрема застосування обмежень, заборон та державного примусу в інформаційній сфері [16, с. [201].

Ю. Стрельцов виділяє загальні та специфічні принципи забезпечення інформаційної безпеки. До загальних принципів належать гуманізм, соціальна справедливість, об'єктивність, ефективність, законність і конституційність, а також баланс між публічністю та професійною таємницею. У ній визначено спеціальні принципи як принцип глобальності, що підкреслює міжнародний характер інформаційних загроз та необхідність комплексного підходу до їх нейтралізації [24, с. 154].

Колектив авторів навчального посібника «Методи захисту інформації» (Ю. Уфімцев, В. Буянов, Є. Єрофєєв та ін.) акцентує увагу на законності заходів, що застосовуються для виявлення та попередження злочинів в інформаційній сфері. Вони також вважають важливими принципами постійне вдосконалення методів захисту інформаційних систем, економічну доцільність витрат на безпеку та комплексний підхід до захисту інформації [27, с. [401].

Ю. Логунов підкреслює, що основою міжнародного права є Статут

ООН, який посідає найвищу позицію в ієрархії міжнародних норм і регулює ключові аспекти глобальної безпеки, в тому числі інформаційної. ООН визначає мету сприяння соціально-економічному розвитку народів, що безпосередньо пов'язане із забезпеченням безпеки інформаційного простору [17, с. 109].

Загалом інформаційна безпека є невід'ємною складовою національної безпеки, яка впливає на всі сторони державного та суспільного життя: політичну, економічну, соціально-культурну, науково-технічну, оборонну, екологічну тощо. Державна політика інформаційної безпеки має бути спрямована на:

- Захист конституційних прав і свобод громадян;
- збереження культурних, духовних, моральних, інтелектуальних і матеріальних цінностей суспільства;
- Гарантувати інформаційний суверенітет, територіальну цілісність і державну безпеку в політичній, економічній, технологічній та військовій сферах [17, с. [110].

Для формування та ефективного функціонування системи захисту інформації необхідні чітко визначені принципи, які мають бути закріплені на законодавчому рівні. Вони відіграють важливу роль у правовому регулюванні відносин у цій сфері та забезпечують ефективну інтеграцію інформаційної безпеки в загальну систему національної безпеки [17, с. 111].

Національна безпека України забезпечується реалізацією виваженої державної політики, що ґрунтується на відповідних доктринах, концепціях, стратегіях і програмах у сферах політики, економіки, оборони, науки, екології та інформаційних технологій. Це потребує вчасного вжиття заходів, що відповідають масштабам і характеру загроз національним інтересам [3].

На основі проведеного аналізу можна виділити основні принципи інформаційної безпеки, які є ключовими для забезпечення захисту інформаційного простору України:

- Пріоритет прав, свобод і законних інтересів громадян;

- Верховенство права та рівність усіх суб’єктів правовідносин перед законом;
- Відповідальність держави перед громадянами в реалізації інформаційної політики;
- Комплексний підхід до забезпечення інформаційної безпеки;
- Єдність і взаємозв'язок сфер захисту інформаційного середовища;
- Розмежування відповідальності між органами державної влади та органами місцевого самоврядування з питань інформаційної безпеки;
- Активна участь у міжнародних ініціативах та регіональних системах захисту інформації;
- Ефективність, своєчасність та попередження заходів щодо виявлення, запобігання та нейтралізації загроз інформаційній безпеці [15, с. 14].

Отже, проаналізувавши принципи забезпечення інформаційної безпеки в Україні, можна зробити висновок, що запропоновані принципи є основою формування та функціонування національної системи інформаційної безпеки.

Водночас, враховуючи стрімкий розвиток цифрових технологій, зміну загроз та нові виклики глобалізації, необхідно постійно оновлювати та адаптувати принципи інформаційної безпеки відповідно до сучасних умов. Майбутні виклики, пов’язані з розвитком штучного інтелекту, децентралізованих технологій, інформаційної війни та кіберзлочинності, вимагатимуть нових механізмів захисту та вдосконалення існуючих підходів.

Запропоновані принципи дозволяють уникнути фрагментації та хаотичного розвитку національної системи інформаційної безпеки, забезпечуючи єдність підходів, ефективне правове регулювання та координацію між державним, приватним та громадським секторами.

Тому інформаційна безпека є ключовим фактором стабільності держави та суспільства, а її реалізація потребує комплексного стратегічного підходу, орієнтованого на сучасні загрози та глобальні тенденції у сфері інформаційної

політики та технологій.

РОЗДІЛ 2
АНАЛІЗ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА США

2.1 Нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині

Аналізуючи нормативно-правову базу інформаційної безпеки Німеччини, Польщі, Хорватії та Угорщини, варто зазначити, що міжнародно-правові акти містять широкий підхід до трактування інформаційної та мережевої безпеки. Розглядається як здатність інформаційної системи або мережі протистояти впливу загроз певного рівня надійності, зокрема надзвичайних ситуацій, кібератак, зловмисних дій або несанкціонованого втручання, які можуть спричинити порушення конфіденційності, доступності та цілісності інформації.

Загалом інформаційна безпека визначається такими ключовими категоріями:

- Доступність, що передбачає можливість користувача отримати інформацію в потрібний час і в потрібний спосіб.
- Ідентифікація, що включає підтвердження прав доступу суб'єкта до певних інформаційних ресурсів.
- Цілісність, яка передбачає збереження структури та змісту інформації без несанкціонованих змін або пошкоджень.
- Конфіденційність, яка захищає дані від доступу третіх осіб і гарантує безпеку особистої або стратегічно важливої інформації.

Особливий акцент у нормативних актах приділяється правовому регулюванню процедур перехоплення та дешифрування інформації, що стосується як заходів, спрямованих на протидію злочинності, так і захисту персональних даних громадян від несанкціонованого доступу [21, с. 131].

Історично важливим нормативним документом у сфері правового

регулювання доступу до інформації є шведський Акт про свободу преси 1776 р. Цей нормативний акт вперше закріпив право громадян на отримання інформації про діяльність державних органів. У сучасних умовах його положення поширюються не лише на офіційні паперові документи, а й на електронні інформаційні ресурси, що відображають діяльність органів влади.

У ряді європейських країн, зокрема в Нідерландах, Іспанії, Португалії, Австрії, Угорщині, Естонії, Бельгії та Румунії, право громадян на доступ до офіційної інформації закріплено на конституційному рівні. Це означає, що держава гарантує прозорість діяльності влади та створює правові механізми для забезпечення відкритості даних. У Франції, Греції та Італії право громадян на інформацію регулюється спеціальними законодавчими актами.

Варто зазначити, що правове регулювання у цій сфері постійно вдосконалюється у Великій Британії, Німеччині, Естонії, Молдові, Польщі та ряді інших країн. Це свідчить про активну еволюцію механізмів інформаційної безпеки в умовах цифрової трансформації суспільства та необхідності реагування на нові виклики інформаційного середовища.

Варто виділити ситуацію у Швеції та Фінляндії, де, незважаючи на високий рівень інформаційної відкритості, існують законодавчо встановлені обмеження доступу до державної інформації. Це пов’язано з необхідністю захисту державної таємниці, персональних даних та іншої конфіденційної інформації.

Ще однією важливою тенденцією в країнах Європи, як і в Україні, є розробка та впровадження концепцій електронного урядування. Ці концепції базуються на використанні сучасних інформаційних технологій для створення державних інформаційних ресурсів, забезпечення доступу громадян до офіційних даних та покращення комунікації між владою та суспільством.

Наприклад, в Австрії законодавчо закріплено право громадян на доступ до законодавчої бази, але офіційною інформацією володіє державний сектор, а не комерційні структури. Водночас за копіювання та розповсюдження документів може стягуватися плата, яка частково компенсує витрати держави

на утримання інформаційних систем.

Таким чином, аналіз зарубіжного досвіду правового регулювання інформаційної безпеки дозволяє виявити загальні закономірності та відмінності у підходах різних країн до захисту інформаційного простору.

З одного боку, всі країни ЄС працюють над забезпеченням відкритості державної інформації та доступу громадян до офіційних даних. З іншого боку, існують певні обмеження та правові механізми, спрямовані на захист конфіденційних публічних і приватних даних.

Крім того, в останні десятиліття активно розвивається правове регулювання цифрового середовища, яке охоплює такі питання, як електронна комерція, використання цифрових підписів і захист персональних даних.

Значна частина нормативних актів у сфері інформаційної безпеки в зарубіжних країнах стосується електронної комерції та цифрового підпису. Це включає:

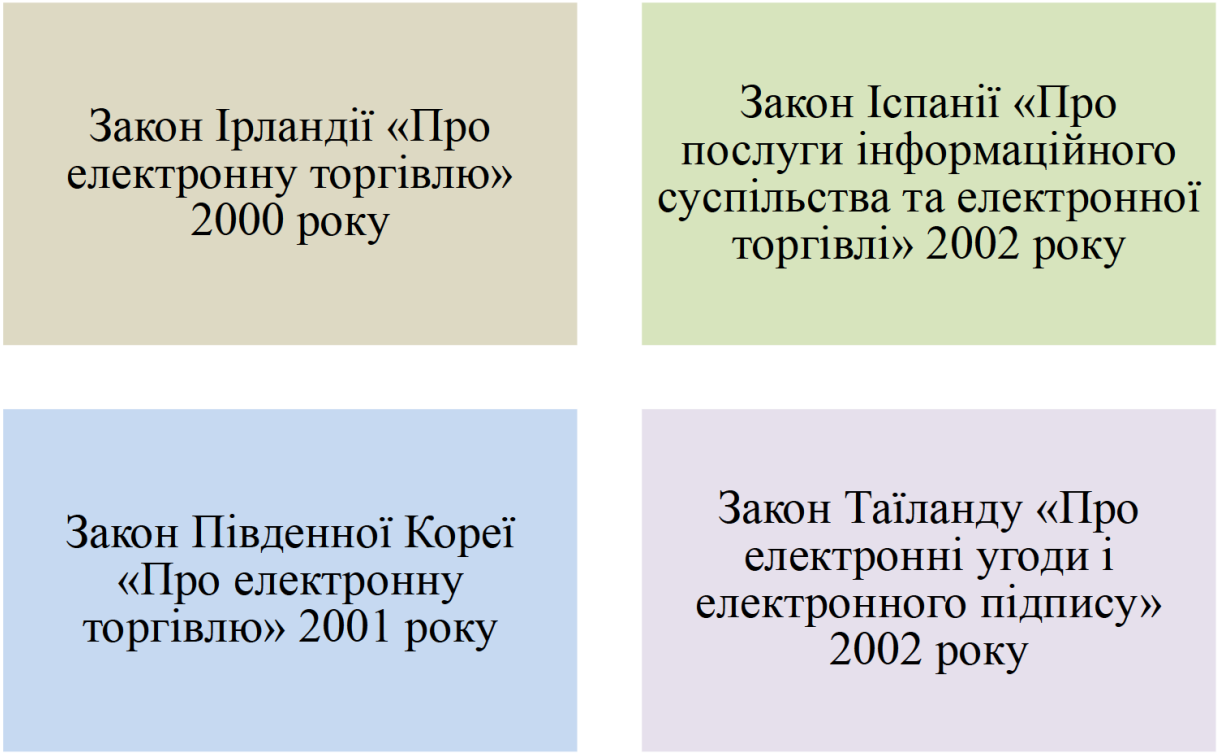
- Забезпечення автентичності цифрових транзакцій;
- Створення безпечного механізму авторизації користувачів;
- Захист персональних і фінансових даних;
- Регулювання відповідальності за кібератаки, злом та неправомірне використання персональної інформації.

Сучасне законодавство Німеччини, Польщі, Хорватії та Угорщини активно адаптується до нових загроз у цифровому середовищі та запроваджує різноманітні механізми забезпечення інформаційної безпеки.

Загалом спостерігається тенденція до гармонізації законодавства європейських країн у сфері інформаційної безпеки. Це пов’язано з необхідністю уніфікації стандартів захисту персональних даних, боротьби з кіберзлочинністю, удосконалення механізмів державного контролю за інформаційним простором та створення ефективних стратегій реагування на кіберзагрози.

Таким чином, досвід правового регулювання інформаційної безпеки в країнах ЄС дозволяє зробити висновок, що успішне функціонування

інформаційних систем неможливе без чіткої законодавчої бази, яка встановлює баланс між відкритістю інформації, захистом інтересів держави та гарантуванням прав громадян в епоху цифрових технологій.



Малюнок 2.1. Звід законів і нормативних актів у сфері інформаційної безпеки зарубіжних країн.

Примітка: Підготовлено автором за джерелом [41].

Аналіз нормативно-правової бази інформаційної безпеки Німеччини, Польщі, Хорватії та Угорщини показує наявність законодавчих актів, спрямованих на регулювання функціонування інформаційних систем, захисту персональних даних, протидії кіберзагрозам та забезпечення безпеки цифрового середовища. У цих країнах питання інформаційної безпеки є пріоритетним напрямком державної політики, оскільки сучасні інформаційні технології є основою функціонування державних установ, підприємств, банківських установ та багатьох інших галузей економіки. Будь-який збій у роботі інформаційних систем може мати серйозні наслідки, включаючи втрату конфіденційних даних, збої у фінансових операціях, збої в роботі державних установ та критичної інфраструктури. У зв’язку з цим уряди цих країн

приділяють велику увагу розробці нових правових механізмів, які дозволять їм своєчасно реагувати на виклики сучасного інформаційного простору.

Правове регулювання інформаційної безпеки передбачає не лише запобігання злочинам у цифровому середовищі, а й забезпечення прав громадян на захист їх персональних даних, а також створення умов для безпечного використання інформаційних технологій у повсякденному житті. Наприклад, у Німеччині питання кібербезпеки регулюються низкою законодавчих актів, які встановлюють стандарти захисту інформаційних систем як у державному, так і в приватному секторах. У Польщі особлива увага приділяється безпеці державних інформаційних ресурсів, зокрема баз даних, що містять конфіденційну інформацію. Угорщина прийняла закони, спрямовані на посилення захисту інформаційних мереж, які використовуються в критичних секторах економіки. Хорватія постійно модернізує своє законодавство про цифрову безпеку, що передбачає адаптацію національних норм до вимог ЄС.

Захист персональних даних є одним із ключових аспектів правового регулювання інформаційної безпеки. Важливість цієї теми зумовлена тим, що в сучасному цифровому суспільстві значна частина інформації зберігається в електронному вигляді, а технології збору та обробки даних постійно вдосконалюються. Наприклад, в Європейському Союзі діє Загальний регламент захисту даних (GDPR), який встановлює жорсткі правила збору, зберігання та обробки персональних даних громадян. Цей документ є обов’язковим для всіх країн ЄС, включаючи Німеччину, Польщу, Хорватію та Угорщину. Прийняття цього регламенту стало відповіддю на зростаючі ризики, пов’язані з витоком особистої інформації, кіберзлочинністю та незаконним використанням даних у комерційних цілях.

В Іспанії в 1999 році було схвалено Органічний закон про захист персональних даних, який регламентує порядок збору, обробки та передачі інформації про громадян. Закон визначає, що загальнодоступними джерелами можуть бути телефонні довідники, списки кандидатів на виборні посади,

професійні реєстри, а також офіційні вісники та публікації в ЗМІ. Інші європейські країни також мають подібні законодавчі акти, які регулюють використання персональних даних, а також визначають відповідальність за їх неправомірне використання. У Польщі, наприклад, прийняті спеціальні правила, що регулюють зберігання даних у банківській системі, медичних установах, навчальних закладах та державних установах. В Угорщині особлива увага приділяється контролю за цифровими транзакціями, які здійснюються в Інтернеті, особливо у сфері електронної комерції та онлайн-банкінгу.

В Україні питання захисту персональних даних регулює Закон «Про захист персональних даних», прийнятий у 2010 році. Документ визначає основні принципи обробки персональних даних, порядок їх зберігання, а також зобов'язання державних і приватних організацій у сфері захисту інформації. Крім того, важливим кроком до посилення правового захисту інформації про особу стало приєднання України до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року. Це дозволило Україні гармонізувати своє законодавство з європейськими стандартами, що сприяло підвищенню рівня безпеки цифрових ресурсів та запровадженню більш ефективних механізмів захисту інформації громадян.

Окрім питань захисту персональних даних, значна увага приділяється правовому регулюванню діяльності в Інтернеті. У сучасних умовах кіберпростір став важливою складовою глобальної економіки, соціальної комунікації та політичного життя. Разом з розвитком інформаційних технологій з'явилися нові ризики, пов'язані з поширенням дезінформації, цифровим шпигунством, кіберзлочинністю та онлайн-тероризмом. Щоб протистояти цим загрозам, країни ЄС впроваджують нові правові механізми моніторингу діяльності онлайн-платформ, посилюють боротьбу з незаконним контентом і захищають права користувачів на безпечне користування Інтернетом.

У 2001 році Європейська комісія опублікувала документ «Мережева

та інформаційна безпека: європейський політичний підхід», у якому визначено основні принципи інформаційної безпеки в країнах ЄС. Документ передбачає впровадження єдиних стандартів кіберзахисту, створення механізмів реагування на загрози в цифровому середовищі та розширення співпраці між державами-членами у сфері кібербезпеки. Програма «Безпечніший Інтернет», яка діє з 1999 року, спрямована на боротьбу з незаконним контентом, запобігання шахрайству в Інтернеті, протидію кібербулінгу та підвищення цифрової грамотності серед населення.

У 2009 році Європейський Союз оприлюднив документ «Захист Європи від широкомасштабних кібератак», який визначає стратегічні напрямки посилення кіберзахисту та підвищення рівня безпеки цифрового середовища. У документі зазначається, що кіберзагрози можуть завдати значної економічної та політичної шкоди, і тому країни-члени ЄС повинні спільно розробити нові методи боротьби з кібератаками. Крім того, у 2013 році Генеральна Асамблея ООН прийняла Резолюцію «Про право на приватність в епоху цифрових технологій», яка встановила необхідність захисту цифрових прав громадян і забезпечення конфіденційності особистої інформації.

Законодавство Німеччини є одним із найрозвиненіших у сфері інформаційної безпеки. У 1997 році було прийнято Закон про захист телекомунікаційних даних (TDPA), який регулює збір, обробку та використання персональних даних. Крім того, у 2005 році в країні набув чинності Закон про свободу інформації , який гарантує громадянам право отримувати офіційні дані від державних органів. З 2010 року в Німеччині діє Федеральна служба інформаційної безпеки, яка координує заходи у сфері кіберзахисту, аналізує загрози в цифровому середовищі та розробляє нові правові механізми у сфері кібербезпеки.

2.2. Характеристики інформаційної безпеки в державних органах (досвід США)

Аналізуючи досвід Сполучених Штатів Америки щодо забезпечення інформаційної безпеки державних органів, слід зазначити, що національна безпека США, у тому числі інформаційна, регулюється нормативними документами стратегічного рівня. Одним із ключових документів, що визначають безпекову політику держави, є Стратегія національної безпеки США (СНБ), яка розробляється адміністрацією кожного нового президента і поєднує в собі напрями зовнішньої політики, оборони, міжнародних економічних відносин і заходи, спрямовані на забезпечення розвитку країни. Нова версія NSS, опублікована в грудні 2017 року, була однією з найдовших в історії США: її обсяг принаймні вдвічі перевищує попередню версію 2015 року. Це свідчить про зростання значення інформаційної безпеки в загальній структурі національної безпеки США, що зумовлено розвитком цифрових технологій, кіберзагрозами та необхідністю захисту державних інформаційних ресурсів.

Враховуючи важливість інформаційної безпеки в сучасних умовах, особливо цінним є досвід США, оскільки країна є одним із лідерів у сфері інформаційних технологій, цифрової інфраструктури та кібербезпеки. Сполучені Штати першими в світі розробили комплексну систему електронного урядування, яка передбачає широкомасштабне використання інформаційних технологій в державному управлінні, а також запровадили спеціальні механізми захисту інформаційного суверенітету країни, безпеки критично важливих ресурсів і забезпечення захисту даних громадян і державних організацій. Саме в США вперше була розроблена концепція кіберзахисту, яка передбачає комплекс заходів щодо захисту інформаційних систем від зовнішніх і внутрішніх загроз, а також методи реагування на можливі комп'ютерні атаки та кібершпигунство.

Сполучені Штати мають широку систему агентств, відповідальних за

забезпечення інформаційної безпеки, включаючи Агентство національної безпеки (АНБ), Національне управління кібербезпеки Міністерства внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР), Центральне розвідувальне управління (ЦРУ), а також ряд спеціалізованих агентств, які контролюють кіберпростір і забезпечують безпеку державних інформаційних систем. АНБ відповідає за збір, аналіз і обробку інформації, забезпечуючи швидке реагування на потенційні загрози національній безпеці. Національний директорат з кібербезпеки координує діяльність у сфері захисту критичної цифрової інфраструктури, включаючи державні телекомунікаційні мережі, фінансові системи, електроустановки, транспортні системи та інші важливі сектори економіки.

Відмінною рисою кібербезпеки США є тісна взаємодія державних установ з приватним сектором і науковими установами, що дозволяє застосувати комплексний підхід до захисту цифрового середовища. АНБ активно співпрацює з великими корпораціями, що займаються розробкою програмного забезпечення, кібербезпекою та аналізом загроз, а також з дослідницькими інститутами, що спеціалізуються на питаннях інформаційної безпеки. Співпраця держави та приватних компаній у сфері кіберзахисту передбачає розробку спільних програм, спрямованих на моніторинг цифрового простору, виявлення потенційних загроз, запобігання кібератакам та створення ефективних механізмів реагування на цифрові загрози.

Президент США є центральною фігурою у сфері регулювання інформаційної безпеки, що визначає основні напрями розвитку цієї сфери та затверджує ключові нормативні документи, що встановлюють правові основи діяльності державних органів у сфері кіберзахисту. Основні принципи кібербезпеки США сформувалися після Другої світової війни, коли країна зіткнулася з загрозами радянської пропаганди та інформаційного впливу. Тоді були створені перші правові механізми захисту інформаційного простору держави, які згодом стали основою для формування сучасної системи цифрової безпеки.

Законодавча база США у сфері інформаційної безпеки включає низку нормативно-правових актів, прийнятих у різні періоди історії країни. Зокрема, у 1974 році був прийнятий Закон про захист персональних таємниць, який регулював збір, обробку та використання персональних даних громадян. Того ж року було ухвалено закон «Про державну таємницю», який визначає механізми збереження конфіденційної інформації. У 1984 році був прийнятий Закон ЦРУ про свободу інформації, а в 1987 році - Закон про безпеку комп'ютерних систем, який став першим нормативним законом у сфері кібербезпеки. Згодом система регулювання кібербезпеки США зазнала значної модернізації, особливо після терористичних атак 11 вересня 2001 року, коли кіберзахист було визнано пріоритетом національної безпеки.

У 2003 році була реалізована Національна стратегія безпечного кіберпростору, яка визначила основні загрози цифровій безпеці та механізми їх запобігання. У 2011 році була розроблена Міжнародна стратегія кібербезпеки, яка закріпила принципи міжнародного співробітництва у сфері цифрової безпеки та встановила механізми співпраці з іншими державами для протидії кіберзагрозам. У 2013 році була затверджена Стратегія кібербезпеки критичної інфраструктури, яка передбачала створення нових технологічних механізмів захисту інформаційних систем держави. У 2015 році було прийнято Закон «Про обмін інформацією у сфері кібербезпеки», який значно посилив можливості державних органів щодо боротьби з цифровими загрозами.

Під час президентства Барака Обами питання інформаційної безпеки набули особливого значення, а американська цифрова інфраструктура була офіційно визнана стратегічним національним ресурсом, що потребує державного захисту. За цей період було прийнято низку законодавчих ініціатив, спрямованих на посилення кіберзахисту державних органів, бізнесу та громадян. Окрему увагу було приділено питанням захисту персональних даних, запобігання кібератакам та створенню єдиної системи цифрової безпеки, що охоплює всі державні органи та стратегічні об’єкти країни.

Завдяки активній політиці США у сфері інформаційної безпеки країна

стала одним зі світових лідерів у сфері кіберзахисту, а її досвід використовують багато держав для розробки власних стратегій цифрової безпеки. Інформаційна безпека залишається головним пріоритетом національної безпеки Сполучених Штатів, і поточна модернізація правових механізмів і технологічних рішень дозволяє нам ефективно протистояти сучасним кіберзагрозам.



Малюнок 2.2. Основні державні пріоритети стратегії інформаційної безпеки в США

Примітка: підготовлено автором за джерелом [71].

Пріоритети національної інформаційної політики США визначають ключові напрями розвитку цифрової безпеки, впровадження інноваційних технологій та забезпечення контролю над інформаційними потоками, що є критично важливим для підтримки стабільності та конкурентоспроможності країни в глобальному інформаційному середовищі. Основними завданнями інформаційної політики є підтримка наукових досліджень і технологічних розробок у сфері інформаційно-комунікаційних систем, створення сприятливих умов для обміну технологіями між державними науковими установами та приватним сектором, а також активне сприяння інтеграції новітніх технологій у різні сектори економіки. Значна увага приділяється розширенню міжнародного співробітництва у сфері кібербезпеки,

забезпеченню глобальної координації заходів щодо протидії кіберзагрозам та розробці ефективних механізмів захисту інформаційних систем.

Крім того, наголошується на необхідності модернізації та розвитку інформаційної інфраструктури, що включає удосконалення технологічних платформ, підвищення рівня захисту публічних і приватних цифрових систем, розвиток механізмів регулювання інформаційних потоків та запровадження міжнародних стандартів у сфері інформаційної безпеки. Особливу роль відіграє контроль за діяльністю телекомунікаційних компаній, що забезпечують функціонування глобальних комунікаційних мереж, а також вплив на інформаційні системи, що використовуються в національних і міжнародних економічних процесах. Важливим аспектом американської державної політики є забезпечення балансу між конфіденційністю інформації, доступністю цифрових ресурсів для суспільства, комерційним використанням інформаційних технологій і забезпеченням безпеки даних користувачів.

Вагомий внесок у формування сучасної системи кібербезпеки зробила Національна кіберстратегія (NCS), розроблена відповідно до Указу Президента США від 11 травня 2017 року, яка зосереджена на посиленні захисту федеральних інформаційних мереж, а також критичної цифрової інфраструктури. Цей документ визначив ключові принципи розвитку національної інформаційної безпеки, які спрямовані на посилення державного контролю над кіберпростором, підвищення ефективності відомств, які протидіють цифровим загрозам, а також розширення можливостей у сфері кіберзахисту. Однак, незважаючи на продовження попередньої політики, стратегія викликала значну критику з боку політичних опонентів президента США Дональда Трампа, оскільки включала положення про посилення наступальних операцій у кіберпросторі, що могло призвести до міжнародних конфліктів у сфері цифрової безпеки.

Особливо серйозною проблемою для США стала ситуація можливого втручання іноземних держав у виборчі процеси, що стало однією з головних загроз комп'ютерній безпеці країни. Кампанія впливу, яку, за словами

спецслужб США, проводили російські організації, зокрема Агентство інтернет-досліджень, викликала широке обурення громадськості, спричинила політичну полеміку та призвела до широкомасштабного розслідування. Використання соціальних медіа та цифрових платформ для поширення дезінформації, маніпулювання громадською думкою та підтримки певних політичних сил свідчить про фундаментальну зміну підходів до ведення інформаційної війни, яка у XXI столітті стала важливим інструментом впливу на демократичні процеси та національну безпеку.

У світлі цих погроз у 2017 році в США було розпочато розслідування під керівництвом спеціального прокурора Роберта Мюллера. Слідство проаналізувало сотні тисяч документів, провело десятки допитів і вивчило діяльність онлайн-платформ, через які могли здійснюватися інформаційні атаки. У результаті було зроблено висновок, що інформаційна операція, проведена через соціальні мережі, мала на меті вплинути на хід президентських виборів. Водночас офіційного підтвердження змови кампанії Трампа з іноземними структурами виявлено не було, що стало предметом подальших політичних дискусій і суперечок.

Проблеми інформаційної безпеки в Сполучених Штатах зачіпають не лише політичну сферу, а й повсякденне життя громадян, оскільки кібератаки та зловживання персональними даними стали невід'ємною частиною цифрового середовища. У 2018 році різко зросла кількість вірусних атак, розповсюдження шкідливого програмного забезпечення через несертифіковані додатки та викрадення персональних даних, зокрема номерів кредитних карток, адрес електронної пошти та паролів користувачів. Масштаби кібершахрайства та несанкціонованого використання особистої інформації змусили уряд США запустити масштабну програму зміцнення кібербезпеки, яка передбачає оновлення законодавчих норм, посилення контролю за діяльністю цифрових платформ та впровадження сучасних технологій захисту інформації.

Враховуючи вищезазначене, основним завданням уряду США є

розробка комплексної політики інформаційної безпеки, яка передбачає не лише посилення захисту державних структур, а й підвищення обізнаності громадян щодо цифрових загроз. Проблема кібербезпеки потребує консолідованих зусиль державних структур, приватного сектору та наукових організацій для розробки ефективних механізмів захисту інформаційного простору. Сучасний світ все більше залежить від цифрових технологій, а тому питання інформаційної безпеки стає одним із визначальних факторів збереження національного суверенітету, політичної стабільності та економічного розвитку. Для ефективної протидії сучасним викликам у сфері інформаційної безпеки США мають розширити міжнародну співпрацю у сфері кіберзахисту, сформувати нові стандарти захисту інформаційних ресурсів, розробити комплексні рішення для запобігання цифровим атакам, підтримувати високий рівень технічної компетентності державних і приватних структур у сфері кібербезпеки. Крім того, необхідно розробити правові механізми регулювання діяльності цифрових платформ і соціальних мереж, щоб запобігти використанню цих інструментів для маніпулювання громадською думкою, поширення дезінформації та втручання у внутрішні справи держави.

Таким чином Сполучені Штати опиняються в авангарді боротьби за інформаційну безпеку в епоху цифрових технологій, де новітні технології стають не лише джерелом економічного розвитку, а й засобом ведення сучасних війн. Глобальна конкуренція у сфері інформаційних технологій, зростання кількості кібератак та посилення інформаційних загроз вимагають адаптації стратегії кібербезпеки США до нових викликів, що дозволить США зберегти домінуючу позицію у сфері цифрових технологій та інформаційної безпеки.

РОЗДІЛ 3
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1 Адаптація досвіду країн ЄС з інформаційної безпеки

Аналізуючи досвід країн Європейського Союзу у сфері інформаційної безпеки, можна зазначити, що формування ефективної політики у цій сфері є одним із найважливіших завдань сучасних європейських держав. Пошук балансу між державним контролем над інформаційним простором і ринковими механізмами, які сприяють розвитку цифрових технологій, є ключовим викликом для урядів європейських країн. Важливо зазначити, що політика інформаційної безпеки ЄС розроблена з урахуванням принципів демократичного врядування, що передбачає гарантування прав і свобод громадян у цифровому суспільстві. Однак у різних країнах існують певні відмінності в підходах до регулювання цієї сфери. У Північній Європі, наприклад, держави прагнуть мінімізувати державне втручання в інформаційну сферу, зосереджуючись на створенні механізмів саморегулювання контролю. Водночас у країнах Центральної та Південної Європи перевага віддається більш централізованому підходу, що включає державне регулювання та встановлення жорстких правил у сфері інформаційної безпеки.

Проте, незважаючи на відмінності у підходах, усі держави ЄС дотримуються єдиної стратегії, яка базується на необхідності забезпечення безпечного функціонування цифрового простору, захисту персональних даних громадян, запобігання кібератакам та розвитку міжнародного співробітництва у сфері кібербезпеки. Європейська політика у цій сфері спрямована на створення єдиного інформаційного простору, який дотримується принципів відкритості, прозорості та захисту прав людини. При цьому важливим напрямом розвитку є приватизація та лібералізація ринку інформаційно-комунікаційних технологій, що дозволяє приватним компаніям брати участь у

розробці та впровадженні новітніх технологій у сфері інформаційної безпеки.

Особливу увагу слід звернути на систему інформаційної безпеки Франції, яка є частиною загальної стратегії національної безпеки країни. Франція — одна з небагатьох країн, яка закріпила основні принципи інформаційної безпеки в офіційних державних документах на стратегічному рівні. Важливим документом, що визначає основні принципи забезпечення національної безпеки, є так звана «Біла книга про національну оборону та безпеку», яка містить принципи політики безпеки, а також визначає основні напрямки розвитку інформаційної безпеки у Франції. Цей документ неодноразово оновлювався з урахуванням зміни міжнародних та національних викликів, а також появи нових загроз у сфері інформаційних технологій.

Перша «Біла книга» була опублікована в 1972 році і містила основні принципи оборонної політики Франції. Вона була розроблена в роки холодної війни і була зосереджена на питаннях військової безпеки, стратегічного стримування та захисту національних інтересів країни. Цей документ не приділяв особливої уваги інформаційній безпеці, оскільки на той час цей аспект ще не відігравав такої важливої ролі в системі національної оборони. Проте в наступні десятиліття ситуація докорінно змінилася.

Зокрема, у 1994 році було опубліковано другу Білу книгу, яка вже враховувала нові глобальні тенденції, зокрема завершення холодної війни та трансформацію загроз національній безпеці. У цьому документі особливу увагу приділено переходу від класичних методів ведення війни до нових форм міжнародного конфлікту, що передбачає використання інформаційних технологій як засобу впливу. Зазначалося, що Франції слід приділяти більше уваги питанням інформаційної безпеки та кіберзахисту, оскільки нові виклики, пов’язані з поширенням цифрових технологій, можуть вплинути на стабільність країни.

Третя версія Білої книги, опублікована в 2008 році, вже містила набагато ширший підхід до питань національної безпеки. У документі були враховані виклики, пов’язані з глобалізацією, боротьбою з міжнародним

тероризмом, розвитком цифрових технологій та їх впливом на міжнародні відносини. Вперше в історії Франції було створено концепцію національної кібербезпеки, яка передбачала об'єднання політики внутрішньої безпеки, зовнішньої політики, економічної політики та оборонної політики в єдину систему для забезпечення національної стабільності. Таким чином, у Франції було офіційно визнано, що інформаційна безпека є такою ж важливою складовою національної безпеки, як і традиційні засоби захисту.

Важливим результатом цієї концепції стало створення Національного агентства з безпеки інформаційних систем (ANSSI), яке займається питаннями кібербезпеки, забезпечує захист державних інформаційних систем і координує заходи щодо протидії кіберзагрозам. Франція також має Національну стратегію кібербезпеки, яка спрямована на підвищення рівня захисту публічних і приватних інформаційних ресурсів, розширення міжнародного співробітництва у сфері кіберзахисту та запровадження нових стандартів захисту цифрового середовища.

Сьогодні Франція є однією з найактивніших європейських країн у сфері інформаційної безпеки, а її досвід використовується в багатьох інших країнах ЄС. Водночас сучасні виклики, серед яких зростання кількості кібератак, використання інформаційних технологій для ведення інформаційних воєн, підвищення ролі соціальних мереж у політичних процесах, вимагають подальшого вдосконалення політики інформаційної безпеки. Уряд Франції активно працює над новими законодавчими ініціативами, спрямованими на посилення кібербезпеки та забезпечення захисту національних інтересів у цифровому середовищі.

Отже, аналізуючи досвід Франції у сфері інформаційної безпеки, можна зробити висновок, що ця країна однією з перших у Європі офіційно закріпила концепцію інформаційної безпеки на стратегічному рівні, включивши її до загальної системи національної оборони. Їх досвід надзвичайно важливий для інших держав ЄС, оскільки демонструє ефективні підходи до формування державної політики у сфері кібербезпеки. Розвиток

цифрових технологій та їх вплив на суспільство створюють нові виклики, і Франція продовжує вдосконалювати свою систему захисту інформаційного простору, активно співпрацюючи з європейськими та міжнародними партнерами.

Розробка нової стратегії національної безпеки Франції була безпосередньо пов'язана зі змінами глобального середовища, що вимагало перегляду підходів до забезпечення стабільності та суверенітету країни. Глобалізація, яка охопила більшість сфер суспільного життя, суттєво змінила принципи функціонування міжнародних відносин, зробивши їх менш передбачуваними та більш нестабільними. Це створило передумови для появи нових загроз, які виходять за рамки традиційних військових викликів і включають широкий спектр кібернетичних, інформаційних та економічних ризиків. Таким чином, національна безпека більше не сприймається виключно у військовому контексті, а стала багатофакторною системою, яка охоплює економічну, соціальну, інформаційну та технологічну стабільність держави. У 2009 році в рамках перегляду підходів до політики безпеки Франції концепція «стратегії національної безпеки» була офіційно включена до Кодексу оборони країни, що створило основу для подальшого вдосконалення системи державного управління у сфері безпеки.

У Білій книзі з національної безпеки 2008 року особливу увагу приділено питанням інформаційної безпеки, які на той час стали пріоритетними у зв’язку з активним поширенням цифрових технологій та зростанням кількості кіберзагроз. Документ містить аналіз ризиків, пов’язаних з функціонуванням інформаційних систем, засобів масової комунікації та цифрових мереж, що використовуються державними та приватними структурами. Було визнано, що глобальний взаємозв’язок інформації створює додаткові вразливості, які можуть бути використані для здійснення кібератак, інформаційного саботажу та маніпулювання суспільною свідомістю. Було особливо підкреслено, що інформаційна інфраструктура сучасного суспільства охоплює ключові аспекти економічного та соціального життя, зокрема фінансовий сектор, транспортну

систему, охорону здоров'я, оборонну промисловість та державне управління. Тому будь-який збій у функціонуванні інформаційних систем може мати значні наслідки для стабільності держави та функціонування основних соціальних інститутів.

Залежність від інформаційних технологій є одночасно і ключовою перевагою сучасного світу, і серйозною загрозою для соціальної безпеки. У White Paper зазначається, що неконтрольоване поширення цифрових технологій може стати каталізатором розвитку нових форм кіберзлочинності, стратегічного шпигунства, кібератак і навіть масштабного цифрового саботажу, який можуть організовувати як державні структури, так і недержавні актори. Особливу увагу було приділено загрозі культурної експансії через цифрові платформи, соціальні мережі та ЗМІ, що може призвести до маніпулювання громадською думкою, поширення дезінформації та послаблення національної ідентичності. У цьому контексті Франція усвідомила необхідність створення ефективної системи протидії інформаційним загрозам, яка стала одним із ключових стовпів її стратегії національної безпеки.

У 2013 році вийшла четверта версія Білої книги з національної оборони та безпеки, яка продовжила розвиток концепції комплексного підходу до забезпечення безпеки країни. Документ містить оновлені положення щодо кібербезпеки, включаючи нові методи запобігання та реагування на цифрові загрози, а також заходи захисту критично важливих інформаційних систем. Було визнано, що інформаційна безпека є невід'ємною частиною загальної оборонної стратегії держави, а ефективне функціонування цифрових систем є важливою умовою збереження політичної стабільності, економічного розвитку та соціального добробуту.

У 2017 році під керівництвом президента Еммануеля Макрона було опубліковано п'яту версію стратегічного документу: «Стратегічний огляд оборони та національної безпеки». Цей документ містив розширений погляд на інформаційні загрози та визначав нові підходи до їх нейтралізації. Зазначалося,

що в сучасному світі кіберпростір став однією з ключових арен міжнародного протистояння, де держави та недержавні суб'єкти ведуть інформаційні війни методами кібератак, пропаганди, дезінформації та психологічного впливу. У документі наголошується, що деякі кіберзагрози можна кваліфікувати як акти збройної агресії, що потребує відповідної відповіді на військово-політичному рівні.

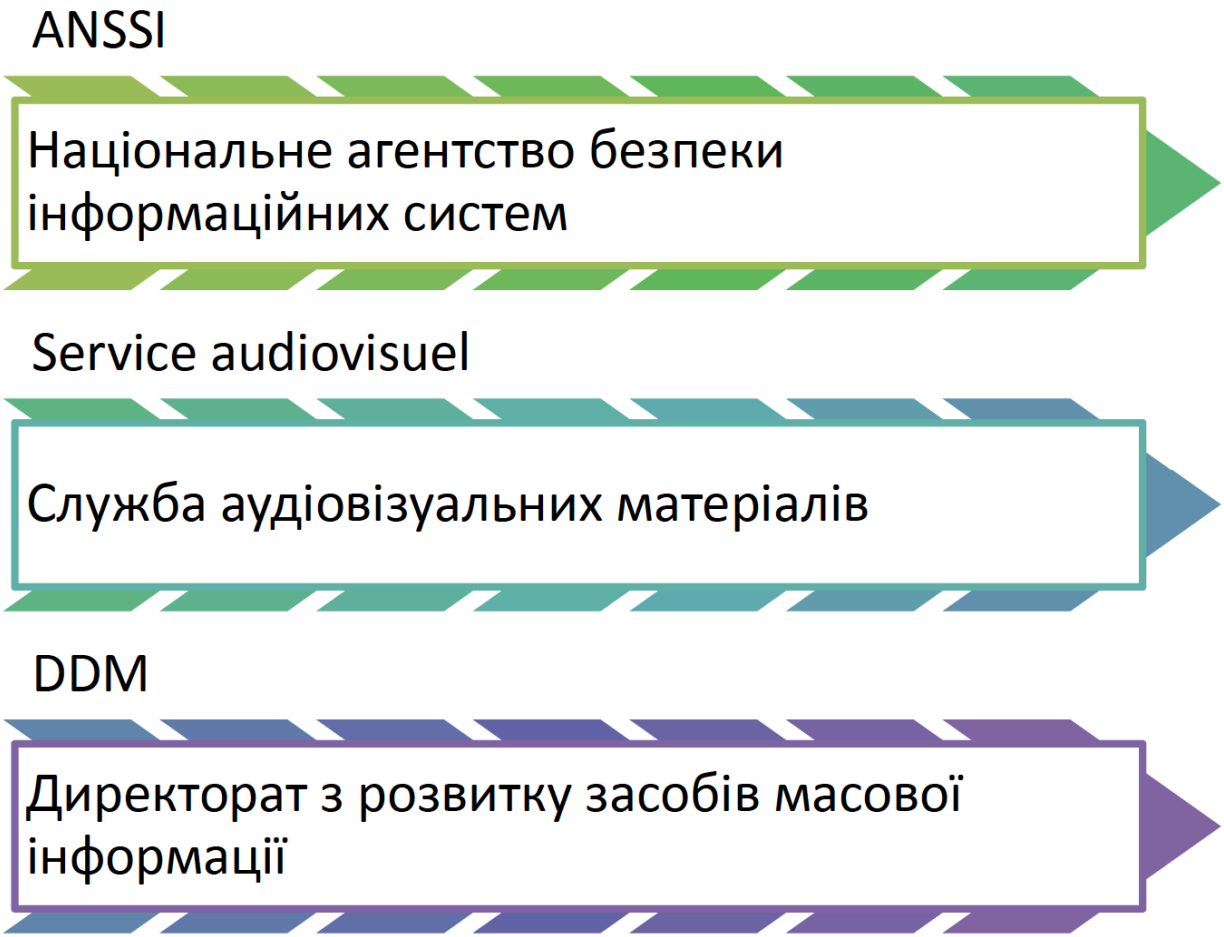
Однією з основних проблем у боротьбі з кіберзагрозами є складність їх ідентифікації та розмежування традиційних методів пропаганди, маніпулювання масовою свідомістю та деструктивних дій у кіберпросторі. Використання змішаних методів впливу, коли кібератаки поєднуються з інформаційними кампаніями, спрямованими на підрив стабільності, створює додаткові виклики національній безпеці. Саме тому Стратегічний огляд наголошує на необхідності комплексного підходу до планування операцій у цифровому просторі та розробки нових інструментів для виявлення та нейтралізації загроз.

Одним із важливих аспектів інформаційної безпеки, визначених у документі, є підготовка французької армії до проведення операцій у кіберпросторі на всіх рівнях, від стратегічного до тактичного. Операції в цифровому середовищі стали одним із нових напрямків військової діяльності, який передбачає використання кіберзброї для захисту держави та її інтересів. Франція офіційно визнала можливість ведення кібервійни в рамках оборонної стратегії, яка включає як оборонні, так і наступальні операції в цифровому середовищі. Це стало важливим елементом загальної політики кібербезпеки країни, яка передбачає активну протидію загрозам як з боку державних, так і недержавних суб'єктів.

На виконання положень стратегічних документів прийнято закон «Про військове планування на 2019-2025 роки», який містить конкретні заходи щодо підвищення рівня кібербезпеки в країні. Одним із найсерйозніших викликів кібербезпеці Франції є кіберджихадизм: використання цифрових платформ, соціальних мереж та онлайн-ресурсів для просування радикальних ідей,

вербування нових членів терористичних організацій та координації терористичної діяльності. Французький уряд активно працює над створенням системи протидії таким загрозам, включаючи блокування екстремістських ресурсів, моніторинг онлайн-простору та розробку програм протидії пропаганді.

Спеціалізовані установи відіграють важливу роль у системі інформаційної безпеки Франції, включаючи Національне агентство безпеки інформаційних систем (ANSSI), Аудіовізуальну службу, Міжвідомчу дирекцію інформаційно-комунікаційних систем (DISIC) і дирекцію розвитку ЗМІ. Ці установи забезпечують реалізацію державної політики кібербезпеки, координують діяльність із захисту інформаційних ресурсів та розробляють нові механізми запобігання загрозам для інформації.



Малюнок 3.1. Система захисту інформації у Франції

Примітка: Підготовлено автором за джерелом [51]

Національне агентство з безпеки інформаційних систем (ANSSI) є

ключовим елементом системи кібербезпеки Франції. Це спеціалізована служба, створена у 2009 році, підпорядкована Генеральному секретаріату оборони та національної безпеки та відповідає за розробку, впровадження та контроль заходів інформаційної безпеки. Враховуючи стрімкий розвиток цифрових технологій, а також зростаючий рівень загроз у кіберпросторі, ANSSI відіграє важливу роль у посиленні стійкості критично важливої державної інформаційної інфраструктури, захисті стратегічних комунікаційних мереж і боротьбі з потенційними кібератаками. Основним завданням агентства є розробка та реалізація державної політики у сфері захисту інформаційних систем, забезпечення їх стабільності, своєчасне реагування на загрози та координація дій державних і приватних структур у разі виникнення кризових ситуацій.

Одним із головних завдань ANSSI є підвищення ефективності управління цифровими ресурсами та координація діяльності державних установ і приватного сектору у сфері комп'ютеризації. Оскільки інформаційна безпека охоплює широкий спектр тем, включаючи кіберзахист, захист персональних даних, безпеку зв'язку та стратегічне управління інформаційними ресурсами, діяльність ANSSI поширюється на різні рівні, від захисту інформаційних систем місцевого самоврядування до участі в міжнародних програмах кібербезпеки. Агентство також займається розробкою правових і технічних стандартів для підвищення загального рівня безпеки державних інформаційних систем та моніторингом дотримання цих стандартів державними органами та об'єктами критичної інфраструктури.

ANSSI впроваджує комплекс заходів для виявлення, аналізу та запобігання кіберзагрозам. Це включає постійний моніторинг кіберпростору для виявлення потенційних атак, виявлення аномальної активності в урядових мережах і розробку рекомендацій щодо посилення безпеки інформаційних ресурсів. Відомство також розслідує кіберінциденти та координує діяльність державних і приватних структур у разі масових атак на інформаційну інфраструктуру. Велика увага приділяється створенню та підтримці надійних

технологічних рішень, які сприяють розвитку цифрової економіки, а також підтримці національної кіберекосистеми. Одним із найважливіших напрямків діяльності ANSSI є сертифікація програмно-апаратних рішень для захисту інформаційних систем, що дозволяє мінімізувати ризики використання вразливих або небезпечних технологій.

Важливу роль у забезпеченні інформаційної політики держави відіграє аудіовізуальна служба, яка діє під егідою Президента Франції. Вона відповідає за розвиток і підтримку аудіовізуальних платформ, які використовуються Президентом для спілкування з громадськістю та міжнародним співтовариством. До основних завдань служби входить організація виступів Президента, їх технічне забезпечення та розповсюдження різними інформаційними каналами як всередині країни, так і за кордоном. Крім того, у службі є відділ фотозйомки, який документує офіційні події та діяльність Президента, веде архів, взаємодіє зі ЗМІ. Важливою частиною їх роботи є моніторинг інформаційного простору та аналіз медіа-контенту для оцінки громадської думки, що дозволяє коригувати інформаційну політику в режимі реального часу.

Міжвідомчий директорат інформаційних та комунікаційних систем (DISIC), створений у 2011 році, відіграє ключову роль у забезпеченні ефективного функціонування інформаційних систем у державному управлінні Франції. Його діяльність спрямована на розробку та впровадження комплексних рішень для оптимізації інформаційних потоків між державними органами та забезпечення безпечного зв’язку в державних структурах. Департамент відповідає за розробку стратегічних ініціатив, спрямованих на покращення координації між міністерствами у сфері цифрових технологій, стандартизацію інформаційних процесів та впровадження єдиних державних систем управління даними. DISIC забезпечує централізований контроль над державними інформаційними ресурсами, забезпечуючи ефективний моніторинг тенденцій кібербезпеки та швидке реагування на потенційні загрози.

У Німеччині основним законом у сфері інформаційної безпеки є Закон «Про посилення безпеки систем інформаційних технологій», прийнятий у 2015 році. Цей нормативний акт визначає основні принципи захисту критичної інформаційної інфраструктури, яка включає енергетичний сектор, телекомунікації, транспорт, охорону здоров’я, водопостачання, фінансовий сектор та інші важливі галузі. Закон надає Федеральному відомству з інформаційної безпеки (BSI) центральну роль у забезпеченні кіберзахисту, особливо в сферах державного управління, приватного сектора та оборонного комплексу. Основною функцією BSI є моніторинг загроз, розробка стратегій реагування та підтримка високого рівня безпеки інформаційних систем.

Критична інфраструктура потребує особливого захисту, оскільки її дестабілізація може мати серйозні наслідки для суспільства. Згідно з чинним законодавством, компанії в критично важливих секторах економіки зобов'язані дотримуватися суворих стандартів безпеки інформаційних систем і періодично подавати звіти про стан їх захисту до Федерального управління безпеки інформації. Крім того, BSI координує дії у разі масштабних кібератак і відповідає за впровадження заходів, спрямованих на зниження ризиків у цифровому просторі. У 2019 році Федеральне міністерство внутрішніх справ Німеччини опублікувало оновлений проект закону про кібербезпеку, який планує посилити компетенцію BSI, запровадити додаткові механізми контролю та розширити перелік правопорушень, пов’язаних з інформаційною безпекою.

Кіберзахист у Німеччині також забезпечує Бундесвер. Відділ комп’ютерних мереж та інформаційних операцій Командування стратегічної розвідки виконує завдання з виявлення та аналізу потенційних загроз у цифровому середовищі. Крім того, розвідувальна система SAR-Lupe, що складається з п'яти супутників, дозволяє в режимі реального часу відстежувати військово-політичну ситуацію, забезпечуючи високоточну розвідку незалежно від погодних умов і часу доби. Це дає Німеччині можливість контролювати стратегічно важливі території та швидко реагувати на потенційні загрози.

Таким чином, розвиток систем інформаційної безпеки у Франції та Німеччині демонструє комплексний підхід до захисту критичної інфраструктури, який включає як державні, так і приватні ініціативи. Обидві країни активно працюють над вдосконаленням механізмів кіберзахисту, впровадженням нових стандартів безпеки та підвищенням рівня координації між державними органами. Це дозволяє нам ефективно протистояти сучасним загрозам і забезпечувати стабільність цифрових систем у мінливих умовах міжнародної безпеки.

Системи інформаційної безпеки в країнах Європейського Союзу характеризуються багаторівневим підходом до захисту критичної інфраструктури та державних інформаційних ресурсів. Вони базуються на взаємодії державних установ, приватного сектору та міжнародних структур. Франція та Німеччина є одними з лідерів у цій сфері, їхні уряди приділяють особливу увагу забезпеченню кіберстійкості та впровадженню сучасних методів захисту цифрових активів. Хоча кожна країна має власну модель інформаційної безпеки, є спільні характеристики, які визначають загальні принципи роботи цієї системи.

Французька модель інформаційної безпеки базується на централізованому підході, при цьому основні функції контролю, нагляду та регулювання зосереджені в Національному агентстві безпеки інформаційних систем (ANSSI). Це агентство відіграє ключову роль у забезпеченні безпеки державних установ, критичної інфраструктури та стратегічно важливих компаній. Основним завданням є розробка нормативно-правової бази, спрямованої на підвищення рівня кібербезпеки, створення механізмів реагування на загрози та моніторинг стану безпеки інформаційних систем у державному та приватному секторах. Крім того, ANSSI бере участь у сертифікації програмного забезпечення, що використовується в критично важливих інформаційних системах, а також проводить аудити та оцінку ризиків кіберзагроз.

Характерною рисою французької системи є активна співпраця держави з

приватними компаніями, що працюють у сфері інформаційних технологій. Уряд Франції розуміє, що ефективний захист цифрової інфраструктури неможливий без залучення комерційних компаній, тому ANSSI проводить спільні навчання та навчання з великими корпораціями, фінансовими установами та операторами телекомунікаційних мереж. Одним із ключових напрямів діяльності агентства є формування культури кібербезпеки у громадян та компаній, що дозволяє мінімізувати ризики, пов'язані із загрозами інформації. Важливим елементом є розробка стратегічних документів, які визначають довгострокові напрями розвитку інформаційної безпеки у Франції та передбачають адаптацію до нових видів кібератак і технологічних викликів.

Німецька модель інформаційної безпеки, на відміну від французької, є децентралізованою, значна частина повноважень у цій сфері передана різним державним і військовим структурам. Ключовим органом, відповідальним за кібербезпеку, є Федеральне відомство з інформаційної безпеки (BSI), яке координує заходи щодо захисту інформаційних систем державних установ, приватного сектору та критичної інфраструктури. Водночас у Німеччині є спеціалізовані військові підрозділи, які займаються комп'ютерною розвідкою та кібероперaціями, зокрема Управління інформації та комп'ютерних мереж Бундесверу.

Німецька система кібербезпеки зосереджена на розвідці та проактивному виявленні загроз. Військові структури беруть активну участь у моніторингу інформаційного простору, виявленні потенційних атак та розробці стратегій реагування. Крім того, BSI працює над удосконаленням законодавства, що регулює кібербезпеку, а також впровадженням міжнародних стандартів із захисту інформації. Одним із основних напрямків управлінської діяльності є підвищення кіберстійкості державних органів та підготовка до потенційних кібератак з боку державних чи недержавних суб'єктів.

Важливою складовою німецької стратегії інформаційної безпеки є формування нормативної бази, яка зобов'язує великі компанії та операторів критичної інфраструктури впроваджувати ефективні механізми захисту від

кіберзагроз. Законодавство вимагає обов'язкової сертифікації інформаційних систем, аудиту безпеки та періодичного тестування на вразливості. Це дозволяє підвищити загальний рівень захисту інформаційних ресурсів та забезпечити належний рівень безпеки в умовах цифрової трансформації.

Незважаючи на відмінності у підходах до інформаційної безпеки у Франції та Німеччини, обидві країни активно співпрацюють у рамках Європейського Союзу та НАТО. Європейська політика кібербезпеки передбачає гармонізацію правил і створення єдиної системи реагування на кіберзагрози. Важливу роль у цьому процесі відіграє Європейське агентство з кібербезпеки (ENISA), яке координує діяльність з інформаційної безпеки на рівні ЄС та сприяє застосуванню спільних стандартів у цій сфері.

Одним із головних викликів для країн ЄС є збільшення кількості кібератак і дезінформаційних кампаній, спрямованих на підрив довіри до державних інституцій і демократичних процесів. Франція та Німеччина активно працюють над розробкою механізмів протидії гібридним загрозам, які поєднують кібератаки, маніпуляції інформацією та економічний тиск. Як наслідок, уряди цих країн значно інвестують у розвиток кібербезпеки, розширення можливостей державних органів та підвищення рівня підготовки фахівців у цій галузі.

Досвід Франції та Німеччини у сфері інформаційної безпеки демонструє ефективність поєднання державного регулювання та приватної ініціативи для формування стійкої системи захисту цифрових активів. Французька модель, яка фокусується на централізованому контролі та координації дій через ANSSI, дозволяє швидко реагувати на загрози та підтримує високий рівень безпеки інформаційних ресурсів держави. Водночас німецька стратегія, заснована на децентралізованому управлінні та широкому залученні військових структур, передбачає глибоку аналітичну обробку даних, що допомагає запобігти потенційним загрозам.

Обидві моделі мають свої переваги, і їх досвід може бути використаний іншими країнами, які прагнуть посилити власну інформаційну безпеку.

Сучасні тенденції у сфері кіберзахисту вказують на необхідність міжнародної співпраці, обміну інформацією про кіберзагрози та розробки єдиних стандартів кібербезпеки, що дозволить ефективніше протидіяти загрозам у цифровому середовищі.

3.2 Методичні рекомендації щодо підвищення інформаційної безпеки та організації доступу до публічної інформації

Система інформаційної безпеки України стикається з численними викликами, вирішення яких вимагає комплексного підходу. Однією з головних загроз залишається інформаційна агресія, яка проявляється у поширенні дезінформації, маніпулюванні суспільною свідомістю, ослабленні довіри до державних інституцій та спробах дестабілізувати ситуацію в країні. Вплив деструктивної інформації на громадську думку, особливо через соціальні мережі та інші цифрові платформи, став ефективним інструментом для гібридних атак, які використовують зовнішні сили для досягнення власних геополітичних цілей. Маніпулятивні інформаційні кампанії мають довгострокові наслідки, оскільки створюють викривлене сприйняття реальності, що може призвести до соціальної напруги, поляризації суспільства та послаблення механізмів державного управління.

Інформаційна безпека також тісно пов’язана з питанням доступу до публічної інформації, оскільки прозорість державного управління та вільний потік достовірної інформації є ключовими для стабільності суспільства. Проблема полягає в тому, що відсутність дієвих механізмів контролю за поширенням неправдивої інформації ускладнює боротьбу з маніпуляціями та фейковими новинами. У зв’язку з цим важливим кроком до покращення ситуації є підвищення рівня цифрової грамотності громадян, що дозволить їм критично оцінювати інформацію, розпізнавати маніпулятивний контент та уникати впливу деструктивних інформаційних потоків.

Одним із ключових аспектів підвищення інформаційної безпеки є

розробка сучасної законодавчої бази, що відповідає міжнародним стандартам з урахуванням національних особливостей. Законодавство має передбачати не лише механізми захисту від загроз інформації, а й регулювання діяльності ЗМІ, соціальних платформ та цифрових сервісів, які є основними каналами поширення інформації. Особливу увагу необхідно приділити контролю за поширенням контенту, який має ознаки дезінформації, а також забезпеченню прозорості джерел фінансування ЗМІ з метою уникнення впливу іноземних агентів у національному інформаційному просторі.

Захист інформаційної інфраструктури також є важливим компонентом загальної стратегії інформаційної безпеки. Оскільки значна частина державних процесів, фінансових операцій і критично важливих послуг працюють на цифрових платформах, забезпечення кібербезпеки має бути пріоритетом. Україна вже впроваджує заходи щодо посилення захисту державних інформаційних ресурсів, але наступними кроками має бути розширення співпраці з міжнародними організаціями та партнерами, які мають великий досвід у цій сфері. Створення спільних платформ для обміну інформацією про кіберзагрози та розвиток національної системи моніторингу та реагування на кіберінциденти дозволить значно знизити ризики атак на критичну інфраструктуру.

Ще одним важливим напрямком є інтеграція України в міжнародний інформаційний простір, що передбачає активну взаємодію з європейськими та євроатлантичними структурами. Це не лише сприятиме підвищенню рівня інформаційної безпеки, а й дозволить Україні впровадити найкращі практики у сфері захисту інформації, кібербезпеки та боротьби з дезінформацією. Важливою складовою цієї інтеграції є розширення співпраці з НАТО та Європейським Союзом в обміні інформацією, підготовці фахівців з кіберзахисту та розвитку спільних механізмів реагування на кіберзагрози.

Одним із пріоритетів інформаційної безпеки є розвиток національної інформаційної інфраструктури, яка має гарантувати ефективний контроль інформаційних потоків усередині країни. Важливо створювати власні

технологічні платформи, які можуть стати альтернативою іноземним сервісам, особливо в таких стратегічно важливих сферах, як електронний уряд, фінансові операції, обробка персональних даних і медіа-контент. Впровадження сучасних технологій безпеки, включаючи шифрування даних, методи біометричної автентифікації та блокчейн-рішення, знизить ризики витоку інформації та кіберзлочинності.

Одним із головних викликів кібербезпеки залишається протидія російській кіберагресії, яка спрямована на дестабілізацію ситуації в країні та підрив довіри до державних інституцій. Російські інформаційні атаки включають широкий спектр методів, включаючи поширення фейкових новин, втручання у виборчі процеси, дискредитацію українського військового та політичного керівництва, використання соціальних мереж для координації протестних рухів та поширення антиукраїнських наративів. Україна активно працює над розробкою механізмів протидії цим загрозам, у тому числі шляхом блокування деструктивних ресурсів, моніторингу медіапростору та впровадження заходів щодо підвищення медіаграмотності населення.

Одним із ефективних методів боротьби з інформаційними загрозами є стратегічні комунікації, які дозволяють державі формувати власні наративи протидії дезінформації. Важливою складовою стратегічних комунікацій є налагодження ефективної взаємодії державних органів, ЗМІ, громадянського суспільства та міжнародних партнерів. Це дозволить своєчасно виявляти та нейтралізувати загрози в інформаційному просторі, а також забезпечувати об’єктивне висвітлення подій, що відбуваються в Україні, на міжнародній арені.

Тому вдосконалення системи інформаційної безпеки потребує комплексного підходу, що включає розвиток законодавчої бази, зміцнення кібербезпеки, інтеграцію в міжнародний інформаційний простір, створення національних технологічних платформ та розробку ефективних механізмів протидії дезінформації. Лише за системного підходу та залучення всіх зацікавлених сторін Україна зможе забезпечити належний рівень

інформаційної безпеки та ефективно захистити свої національні інтереси в цифровому середовищі.

Протидія загрозам в інформаційному просторі є одним із ключових завдань української влади, оскільки інформаційні атаки можуть критично вплинути на національну безпеку, політичну стабільність, економічний розвиток та міжнародний імідж країни. Одним із важливих кроків у цьому напрямку стало створення у 2015 році Міністерства інформаційної політики України. Ця структура взяла на себе завдання координації державної інформаційної політики, розробки стратегій інформаційної безпеки, протидії пропаганді та дезінформації, формування єдиного інформаційного простору. Міністерство працювало над розробкою концепції інформаційної безпеки в Україні, впровадженням механізмів протидії інформаційній агресії та створенням ефективної комунікаційної стратегії держави.

Важливу роль у забезпеченні інформаційної безпеки відіграє також Рада національної безпеки і оборони України. Розроблено низку документів, спрямованих на підвищення рівня захисту інформаційного простору, у тому числі рішення про заходи щодо вдосконалення реалізації державної політики у сфері інформаційної безпеки. Серед ключових напрямків діяльності – запровадження механізмів протидії дезінформації та психологічному впливу, блокування шкідливого контенту, посилення контролю за дотриманням інформаційного законодавства та проведення інформаційних кампаній для підвищення обізнаності населення.

Враховуючи значний рівень загроз із зовнішніх джерел, Україна активно працює над вдосконаленням системи кібербезпеки. Відповідні функції виконують декілька державних органів, зокрема Служба безпеки України, Державна служба спеціального зв’язку та захисту інформації, Міністерство внутрішніх справ. Важливим кроком стало створення Національного координаційного центру з кібербезпеки при РНБО, який відповідає за моніторинг ситуації в інформаційному просторі, аналіз кіберзагроз та координацію заходів щодо їх нейтралізації.

Національна система інформаційної безпеки України базується на законодавчих актах, які визначають основи державної політики у сфері захисту інформації. Зокрема, у 2016 році було прийнято Доктрину інформаційної безпеки України, яка визначає основні принципи захисту державної інформації, механізми протидії інформаційній агресії та заходи щодо забезпечення національних інтересів у кіберпросторі.

Сучасні кіберзагрози є серйозним викликом для будь-якої держави, і Україна не є винятком. Кібератаки, спрямовані на порушення критичної інфраструктури, стали одним із ключових методів гібридної війни. Використання шкідливих програм, кібершпигунство та крадіжка конфіденційних даних створюють реальні ризики для національної безпеки. Створення національної системи кібербезпеки є пріоритетним завданням для держави, оскільки належний рівень захисту цифрових систем є ключовим для стабільності державного управління, фінансової системи та інших важливих секторів.

Зіткнувшись із викликами сучасності, Україна активно переймає досвід передових країн у сфері інформаційної безпеки. Наприклад, стратегія кібербезпеки Канади визначає кібершпигунство, кібертероризм і кібератаки на критичну інфраструктуру як серйозні загрози. У країні діє єдина система управління кібербезпекою, яка забезпечує координацію діяльності державних і приватних структур, що працюють у сфері кіберзахисту.

Австрія реалізує свою стратегію кібербезпеки через Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ, який координує діяльність з інформаційної безпеки, розробляє нові методи боротьби з кіберзлочинністю та забезпечує швидке реагування на загрози. Подібна модель діє в Польщі, де Агентство внутрішньої безпеки (AVB) відіграє ключову роль у забезпеченні інформаційної безпеки. Польща також створила Центр криптології при Міністерстві національної оборони, який відповідає за захист державних інформаційних ресурсів і проведення наступальних кібероперацій.

У багатьох країнах кібербезпекою займаються спеціалізовані підрозділи контррозвідки та національні кіберцентри, які відповідають за захист державної інфраструктури, запобігання витокам конфіденційної інформації та боротьбу з кіберзагрозами. Аналіз міжнародного досвіду показує, що ефективні національні системи кібербезпеки передбачають комплексний підхід, який включає правове регулювання, технічний захист, інформаційну освіту та міжнародну співпрацю.

Україна також вживає заходів для створення ефективної системи захисту інформації. Однією з пропозицій є створення Національного центру кібербезпеки, який би підпорядковувався Службі безпеки України. Цей центр має стати координаційним органом, який об’єднає всі ключові структури, відповідальні за інформаційну безпеку. Ще одним важливим напрямком є розвиток власних технологічних платформ, що дозволить зменшити залежність від іноземних рішень у сфері інформаційних технологій.

Національна система інформаційної безпеки має містити механізми ефективної взаємодії державних органів, правоохоронних органів, приватного сектору та громадянського суспільства. Важливо забезпечити високий рівень координації та взаємодії між суб’єктами інформаційної безпеки, що дозволить оперативно реагувати на загрози та мінімізувати їх наслідки.

Сучасні інформаційні виклики вимагають розробки нових стратегій та адаптації до мінливого середовища. Україна має інвестувати у розвиток національної IT-інфраструктури, стимулювати дослідження у сфері кібербезпеки та інформаційної політики, створювати умови для навчання та підготовки фахівців у цій галузі. Важливим завданням є формування ефективної системи кіберзахисту, яка включатиме як технічні рішення, так і законодавчі ініціативи, спрямовані на запобігання загрозам інформації.

Інтеграція України в міжнародну систему інформаційної безпеки зміцнить її позиції на світовій арені та надасть їй доступ до передових технологій у сфері кіберзахисту. Співпраця з країнами ЄС та НАТО є ключовим елементом цієї стратегії, адже міжнародний досвід та ресурси допоможуть Україні

ефективніше протидіяти загрозам у кіберпросторі.

Тому розбудова національної системи інформаційної безпеки має стати одним із пріоритетів державної політики. Комплексний підхід із поєднанням правових, технічних, організаційних та освітніх заходів дозволить створити в Україні ефективну систему захисту інформаційного простору та забезпечення стійкості до зовнішніх і внутрішніх загроз. .

ВИСНОВКИ

У магістерській роботі проведено комплексне дослідження та запропоновано вирішення актуальної наукової проблеми, пов’язаної з державним управлінням процесами інформаційної безпеки в країнах Європейського Союзу та Сполучених Штатів Америки. Основною метою роботи було удосконалення системи інформаційної безпеки України шляхом адаптації позитивного міжнародного досвіду та запровадження ефективних механізмів забезпечення захисту інформаційного простору. У процесі дослідження отримано вагомі результати, що сприяють досягненню поставленої мети, та розроблено ряд практичних рекомендацій. Вони можуть бути використані для оптимізації державної політики у сфері інформаційної безпеки, посилення нормативно-правового регулювання, формування ефективної системи захисту інформації.

У результаті аналізу розкрито поняття інформаційної безпеки як стану захищеності життєво важливих інтересів особи, суспільства та держави, що реалізується за допомогою заходів, спрямованих на запобігання загрозам, пов’язаним з інформаційною діяльністю. Інформаційна безпека забезпечує мінімізацію шкоди, завданої неповною, недостовірною або несвоєчасною інформацією, впливом деструктивної інформації, а також порушенням конфіденційності, цілісності та доступності даних. Крім того, було запропоновано визначити національну систему інформаційної безпеки як сукупність державних, громадських і приватних структур, які взаємодіють з метою захисту інформаційного простору країни. Ця система включає правові, організаційні, технічні та соціальні механізми, спрямовані на запобігання негативним інформаційним впливам, забезпечення безпечної роботи інформаційної інфраструктури та реалізації прав громадян на доступ до достовірної інформації.

Особливу увагу приділено загальним засадам формування та функціонування національної системи інформаційної безпеки. До основних

принципів належать верховенство права, пріоритет прав людини, баланс інтересів особи, суспільства і держави, гарантування громадського контролю за діяльністю органів, відповідальних за інформаційну безпеку. Також важливо забезпечити відповідність заходів безпеки реальним і потенційним загрозам, чіткий розподіл повноважень між державними органами, використання мирних засобів вирішення інформаційних конфліктів та міжнародне співробітництво у сфері інформаційної безпеки. Враховуючи динамічний розвиток інформаційних технологій та процеси глобалізації, було наголошено на необхідності постійного оновлення принципів інформаційної безпеки, їх адаптації до сучасних викликів та інтеграції передового міжнародного досвіду.

Дослідження провело комплексний аналіз нормативно-правової бази інформаційної безпеки в таких країнах, як Німеччина, Польща, Хорватія та Угорщина. Встановлено, що в цих державах проблема захисту інформаційного простору є одним із ключових стратегічних пріоритетів. Підходи до правового регулювання різні, але загальна тенденція полягає у посиленні державного контролю над кіберпростором, розвитку механізмів протидії кіберзлочинності та активному використанні технологічних інструментів для забезпечення безпеки. Європейська політика інформаційної безпеки передбачає створення єдиної системи інформації про загрози, посилення захисту персональних даних, удосконалення регулювання сфери телекомунікацій та запровадження комплексних заходів для підвищення рівня інформаційної безпеки на державному рівні. Особливу увагу приділено використанню електронного підпису та розвитку технологічної інфраструктури для надання державних послуг у цифровому середовищі.

Аналіз американського досвіду організації інформаційної безпеки дозволив виявити ключові особливості функціонування системи захисту інформації США. Сполучені Штати приділяють велику увагу запобіганню загроз з боку іноземних держав, розробці механізмів раннього виявлення кіберзагроз, підготовці фахівців з інформаційної безпеки. Основними завданнями національної кібербезпеки є захист критичної інфраструктури,

покращення моніторингу та реагування на атаки, посилення співпраці з приватним сектором і міжнародними організаціями. Політика Сполучених Штатів у сфері кібербезпеки спрямована на збереження технологічної переваги країни, що дозволяє швидко отримувати, аналізувати та використовувати інформацію для забезпечення національних інтересів. Водночас визначено низку викликів, які стоять перед Сполученими Штатами у цій сфері, зокрема загрози з боку іноземних кіберугруповань, інформаційні атаки та внутрішні проблеми з регулюванням інформаційного середовища. Важливим завданням уряду США є розробка єдиної стратегії інформаційної безпеки, яка підвищить ефективність захисту інформаційного простору.

За отриманими результатами сформульовано основні напрями вдосконалення системи інформаційної безпеки України. Перш за все, необхідно запозичити кращий міжнародний досвід, запровадити сучасні механізми контролю за інформаційним простором, удосконалити законодавство з питань інформаційної безпеки та забезпечити його відповідність міжнародним стандартам. Важливо розвивати національну інформаційну інфраструктуру, посилювати кібербезпеку державних установ, заохочувати співпрацю з міжнародними партнерами та розробляти ефективні механізми захисту персональних даних. Для забезпечення інформаційної безпеки необхідно створити комплексну систему захисту інформаційного простору, що охоплює всі рівні влади, правоохоронні органи, наукові установи, приватний сектор та громадянське суспільство. Важливу роль у цьому процесі відіграє реалізація державної політики, спрямованої на підвищення обізнаності населення у сфері інформаційної безпеки, розвиток інноваційних технологій та створення ефективних механізмів протидії інформаційним загрозам.

Таким чином, у магістерській роботі розкриваються актуальні проблеми забезпечення інформаційної безпеки, аналізується досвід європейських країн та США, визначаються проблеми та виклики, які постають перед Україною у цій сфері та пропонуються конкретні заходи щодо їх вирішення. Запропоновані рекомендації можуть бути використані в процесі розробки національної

стратегії інформаційної безпеки та вдосконалення нормативно-правової бази, що сприятиме створенню ефективної системи захисту інформаційного простору України.

Системи інформаційної безпеки Франції та Німеччини базуються на поглибленому аналізі загроз, які виникають через стрімкий розвиток інформаційно-комунікаційних технологій. У результаті її політика кібербезпеки є цілісною та послідовною, заснованою на компетентних аналітичних оцінках і науково обґрунтованих стратегіях. Основні зусилля зосереджені на постійному розвитку технологій, підготовці персоналу та співпраці з міжнародними партнерами для забезпечення ефективної взаємодії в рамках Європейського Союзу та глобального цифрового простору. Наприклад, важливу роль у системі інформаційної безпеки Франції відіграє Національне агентство з безпеки інформаційних систем (ANSSI), яке займається питаннями державної кібербезпеки, сертифікації програмного забезпечення та управління ризиками в кіберпросторі. У Німеччині подібні функції виконує Департамент інформації та мережевих операцій Бундесверу, надаючи стратегічну інформацію та захищаючи критичну інфраструктуру.

Тенденції розвитку інформаційної безпеки у Франції та Німеччині базуються на концепції технологічного лідерства, активного впровадження інновацій та міжнародної співпраці. Оскільки сучасний світ перебуває в постійній інформаційній динаміці, кібербезпека стає ключовим пріоритетом для держав, які прагнуть забезпечити стабільність власної цифрової інфраструктури. Деякі країни активно розробляють проекти стратегій інформаційної безпеки, пристосовуючи їх до власних загроз і викликів. Україна також не залишається осторонь цього процесу, оскільки розвиток її системи національної безпеки тісно пов’язаний з необхідністю створення ефективної інформаційної безпеки як ключової підсистеми загальної архітектури безпеки держави.

Забезпечення належного рівня інформаційної безпеки в Україні є невід’ємною складовою побудови інформаційного суспільства. Створення

ефективної Національної системи інформаційної безпеки вимагає участі всіх державних органів, пов’язаних із безпекою даних, кіберзахистом та боротьбою з дезінформацією. Ключову роль у цьому процесі відіграватимуть підрозділи СБУ, МВС та Державної служби спеціального зв’язку та захисту інформації. Важливу координуючу роль відіграватиме Рада національної безпеки і оборони України. Одним із ключових викликів розвитку системи інформаційної безпеки є необхідність забезпечення ефективної взаємодії державних органів, відповідальних за інформаційну безпеку, а також координації їх спільної діяльності для досягнення синергії.

Шляхи досягнення інформаційної безпеки в Україні пов’язані з формуванням комплексного підходу до створення безпечного інформаційного простору. Для цього необхідно розробити чітку законодавчу та нормативну базу, яка регулює функціонування інформаційної сфери, визначає відповідальність за поширення дезінформації та передбачає механізми запобігання маніпулюванню громадською думкою. Важливим кроком у цьому напрямку стало прийняття Доктрини інформаційної безпеки України, яка окреслює стратегічні засади розвитку кібербезпеки держави.

Крім того, необхідно створити сприятливі умови для масового впровадження сучасних інформаційно-комунікаційних технологій, підтримувати інновації у сфері кіберзахисту та сприяти розширенню державних ініціатив, спрямованих на захист критичної інформаційної інфраструктури. Важливим аспектом є підвищення інформаційної грамотності громадян. Проведення освітніх вебінарів, спеціалізованих майстер-класів та дослідницьких проектів сприятиме підвищенню обізнаності населення про основні загрози та методи їх запобігання.

Для ефективного функціонування Національної системи інформаційної безпеки необхідно реалізувати державні програми розвитку кіберзахисту, які передбачатимуть як розширення технічних можливостей державних органів, так і створення нових платформ для моніторингу, аналізу та швидкого реагування на кібератаки. Важливою складовою є співпраця з міжнародними

організаціями, такими як Європейське агентство з кібербезпеки (ENISA), НАТО, а також іншими державами-партнерами, які мають успішний досвід у цій сфері.

Тому побудова ефективної системи інформаційної безпеки в Україні потребує системного підходу, що враховує як національні особливості інформаційного простору, так і кращі практики світового досвіду. Формування законодавчої бази, розвиток технічної інфраструктури, підготовка кваліфікованих спеціалістів, координація міждержавного співробітництва та активна участь громадськості – все це є необхідними умовами для побудови сталої системи інформаційної безпеки, здатної ефективно протистояти сучасним викликам і загрозам.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакіна-Пилявська Л. М. Кримінально-правова охорона інформаційної безпеки: сучасні виклики. *Актуальні проблеми боротьби з корупцією в Україні в умовах воєнного стану.* 2023. URL: https://doi.org/10.36059/978- 966-397-293-0-22 (дата звернення: 9.11.2023).

2. Ананченко О. ГАЙ. Питання формування організаційної структури системи управління інформаційною безпекою підприємства. *Сучасний захист інформації.* 2016. № 1. С. 79-83.

3. Андрощук Р. В., Москаленко Р. Е. Н. Управління інформаційною безпекою військовий :thesis.2021.URL: http://ir.stu.cn.ua/123456789/25338 (дата звернення: 9.11.2023).

4. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України. Дисертація на здобуття наукового ступеня кандидата держуправлінських наук. 25.00.02. Механізми державного управління. Національна академія державного управління при Президентові України. Київ. 2017. 218 стор.

5. Апетик А. Інформаційна безпека. 2019. URL: https://www.prostir . ua/%3Flibrarv%3Dinformatsiinabezpeka-now-vakvh-elementiv-ne-vystachaje+&cd=3&hl=ru&ct=clnk&gl=ua (дата звернення: 9.11.2023).

6. Арістова І. ЕН. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики: монографія. Х.: Нац. ун-т внутрішніх справ імені Маркоса, 2006. 354 с.

7. Артемов В. ю. Управління інформаційною безпекою як неодмінна складова побудови інформаційного суспільства в Україні : автореф. 2009. URL: http://essuir.sumdu.edu.ua/handle/123456789/11939 (дата звернення: 9.11.2023).

8. Бакалинський О. Є.Н. Модель та методи визначення конструктивних характеристик систем управління інформаційною безпекою : автореф. дис...техн.канд. наук. Київ, 2019. 19 с.

9. Безштанка В. Цикл впровадження системи управління інформаційною

безпекою. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* Номер 2006. 2 (13). З. 123-126.

10. Березовська І. А. Суб'єкти інформаційної безпеки в Україні. Наукові записки Львівського університету бізнесу та права. Номер 2013. 10. С. 148-153.

11. Богуш В. М., Юдін О. К. Державна інформаційна безпека. К. : МК-Прес, 2005. 432 с.

12. Бондаренко Н., Ситниченко О. Організаційно-правове забезпечення. Корпоративна інформаційна безпека. *Зовнішня торгівля: економіка, фінанси, право.* 2023. Т. 127, № 2. С. 76-87.URL: https://doi.org/10.31617/3.2023(127)05 (дата звернення: 9.11.2023).

13. Бортейчук Р.Ю. Стратегічне управління державою: сутність та механізми його реалізації. *Економіка і держава.* 2011. № 1. С. 121-125.

14. Бурило Ю. П. Правові форми державного управління інформаційною сферою. *Правознавство: теорія і практика.* 2007. № 8. С. 2-10.

15. Бюріх К. І. Інформаційна безпека України в сучасному кіберпросторі. *Національна безпека і оборона.* 2014. № 10. КОН. 21-27.

16. Вареня Н. М. Щодо методів виявлення терористичних загроз і небезпек. *Верховенство права в процесі державотворення та захисту прав людини в Україні:* тези міжнародної науково-практичної конференції. конференції. (Одеса, 12-13 лютого 2016 р.). Одеса: ГО «Причорноморська правова фундація», 2016. С. 104-108.

17. Вербицька А.М., Дзюба Т.М., Кацалап В.О. Кіберскладова гібридної війни проти України. *Українське суспільство в умовах війни: сучасні виклики та перспективи пацифікації: матеріали Всеукраїнської науково-практичної конференції, Київ. Маріуполь 9 червня 2017 р.* Маріуполь: ДонДУУ. 2017. С. 255-258.

18. Воробйова І. ЕН. Інформаційно-психологічна зброя як самостійний засіб ведення інформаційно-психологічної війни. *Системи озброєння та військова техніка.* 2010. № 1. С. 141-144.

19. Герасименко К. С. Сучасні ознаки загроз «інформаційного тероризму». *Юридичний форум.* 2009. № 3. С. 162-166.

20. Гібридна війна: словом і на практиці: монографія. Донецький національний університет імені Василя Стуса. Низький. всього опубліковано проф. Р. О. Додонова. Вінниця: ТОВ «Нілан-ЛТД». 2017. 412 стор.

21. А. А. Головка Діяльність сучасних ЗМІ в контексті інформаційної безпеки України. *Актуальні проблеми гуманітарних і природничих наук* (Ужгород, 8-9 квітня 2016 р.). Херсон: Editorial Helvética, 2016. С. 85-87.

22. Гончаров М. ЕН. Досвід нормативно-правового забезпечення Інформаційна безпека в країнах Європейського Союзу. *Наше право.* 2023. № 2. С. 144-149. URL: https://doi.org/10.32782/np.2023.2.20 (дата звернення: 9.11.2023).

23. Горбулін, віце-президент; Биченок, чл. Копка, прем'єр-міністр. Актуальні проблеми системного забезпечення інформаційної безпеки в Україні: матеріали міжнародної науково-практичної конференції. *«Форми та методи забезпечення безпеки державної інформації».* К.: Нац. Академічний. Служба безпеки України. 2008. Сторінка 79 85.

24. Горова С. ЕН. Особа в інформаційному суспільстві: виклики сьогодення: монографія / наук. опубліковано EN. З. Онищенко; НАН України, Національний Банк України носить ім'я Є.Н. Ю. Вернадського. Київ, 2017. 342с

25. Григор'єв В. І. Інформаційна безпека в державному управлінні. *Бібліотекознавство. Документознавство. Інформологія.* 2013. № 4. С. 53-55.

26. Гурковський В. Я. Державне управління розвитком інформаційного суспільства в Україні (історія, теорія, практика): моногр. Київ: Нічого. Світ, 2010. 396 с.

27. Дем'янюк Ю. Організаційно-педагогічні умови підготовки офіцерів-прикордонників за освітньо-кваліфікаційним рівнем магістра управління інформаційною безпекою. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: педагогічні науки.* 2020. Том 19, № 4. Стор. 147-160. URL:

https://doi.org/10.32453/pedzbirnyk.v19i4.263 (дата звернення: 9.11.2023).

28. Дідіковська Г. В., Топчій В. Е. Н. Криміналістичні механізми захисту інформації. *Ірпінський юридичний журнал.* 2023. № 3(12). З. 236-242. URL: https://doi.org/10.33244/2617-4154-3(12)-2023-236-242 (дата звернення: 9.11.2023).

29. Домарєв Д. Є.Н. Методика інформаційно-аналітичного забезпечення управління інформаційною безпекою на основі структурування оцінок : автореф. дис...техн.канд. наук. Київ, 2015. 20 с.

30. Дотримання прав і свобод громадян України на інформацію:Нормативно-правова база та важелі регулювання. Аналітична записка. URL: https://niss.gov.ua/dosHdzhennya/informaciyni- (дата звернення: 9.11.2023).

31. Tierney TY Заходи національної безпеки, прийняті владоюдержавне управління. *Сучасні вектори відновлення та розвитку України на засадах сталості та безпеки.* 2023. URL: https://doi.org/10.54929/conf 21 11 2023-01-03 (дата звернення:

32. Думчиков М. Є.Н. Види органів державної безпеки Інформаційна безпека та характеристика її компетенцій. *Європейські перспективи.* 2023.№ 3.С. 222-227.URL: https://doi.org/10.32782/ep.2023.3.31 (дата звернення: 9.11.2023).

33. Економічне обґрунтування управління корпоративною інформаційною безпекою: тези / І. МЕТРО. Сотник та ін. 2017. URL: http://essuir.sumdu.edu.ua/handle/123456789/54491 (дата звернення:

9.11.2023) .

34. Житко А. О. Кібервійна як складова гібридної війни. *Українська Суспільство в умовах війни: сучасні виклики та перспективи миротворчості:* матеріали Всеукр. науково-практ.конф., м. Маріуполь, 9 червня 2017 р. Маріуполь: ДонДУУ. 2017. С. 263-266.

35. Заплатинський В. М. Логіко-детерміновані підходи до розуміння поняття «Безпека». *Вісник Кам'янець-Подільського національного*

університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. Кам'янець-Подільський: Кам'янець-Подільський нац.ун-т імені Івана Огієнка. 2012. Номер 5. С. 90-98.

36. Захаренко К. Ключові гравці та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків: ХНПУ. 2017. № 48 (частина І). З. 212-219.

37. Згуровський М. КОН. Проблеми інформаційної безпеки в Україні та шляхи їх вирішення. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. Сторінка 120. 10 14.

38. Зеленін В. ЕН. По той бік істини: нейролінгвістичне програмування як зброя інформаційної війни та пропаганди. О. 1. Вінниця: Видавництво «Віндрук». 2014.384с.

39. Золотар О. ІН. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавництво «АртЕк». 2018. 446 стор.

40. Ільницька У. Інформаційна безпека в Україні: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політологія.* Роман. 2. № 1. 2016. С. 27-32.

41. Іоланда Д. Стратегія забезпечення національної безпеки в Україні. *Теоретичні та прикладні питання державотворення.* 2023. № 29. З. 199-201. URL: https://doi.org/10.35432/tisb292023289628 (дата заявка: 9.11.2023).

42. Я Іськів. Підвищити ефективність державної політики у сфері забезпечення економічної, соціальної та інформаційної складових національної безпеки. *Наукові перспективи.* 2023. № 7(37). URL: https://doi.org/10.52058/2708-7530-2023-7(37)-165-172 (дата звернення: 9.11.2023).

43. Я Іськів. Особливості сутності забезпечення національної безпеки. *Теоретичні та прикладні питання державотворення.* 2023. № 27. С. 143-147.URL: https://doi.org/10.35432/tisb272022276823 (дата заявка: 9.11.2023).

44. Кавін С. Нормативно-правове забезпечення інформаційної безпеки

України в контексті її вступу до Європейського Союзу. *Наше право.* 2023. № 3. С. 140-150. URL: https://doi.org/10.32782/np.2023.3.21 (дата звернення: 9.11.2023).

45. За Кавін С. І. Міжнародно-правове регулювання безпеки. Інформаційна безпека в міжнародних організаціях. *Європейські перспективи.* 2023.№ 2.С. 145-155.URL: https://doi.org/10.32782/ep.2023.2.24 (дата звернення: 9.11.2023).

46. Качинський А. Б. Структурно-функціональна модель системи. Забезпечити безпеку інформації та психологічної інформації. *Доповіді НАН України.* 2023. № 1. С. 16-23. URL: https://doi.org/10.15407/dopovidi2023.01.016 (дата звернення: 9.11.2023).

47. Кашуба Н. Аудит інформаційної безпеки телекомунікаційних систем і пристроїв. *Грааль науки.* 2023. № 27.С. 270-272.URL: https://doi.org/10.36074/el-grial-de-la-ciencia.12.05.2023.042 (дата звернення: 9.11.2023).

48. Кириченко М. ЕН. Формування ідеології інформаційного суспільства як чинника динамічного розвитку та безпеки сучасної України XXI ст. *Вісник Львівського університету. Серія «Філософсько-політичні дослідження»: Збірник наукових праць.* 2017. № 12. С. 74-81.

49. Клочко А. Забезпечення інформаційної безпеки в сучасному суспільстві. *Наукові праці Міжрегіональної академії управління персоналом. Політологія та державне управління.* 2023. № 3(63). З. 38-42. URL: https://doi.org/10.32689/2523-4625-2022-3(63)-6 (дата звернення: 9.11.2023).

50. Коваль З. Питання боротьби з інформаційно-психологічними загрозами. України через державне управління. електрон. наук. професія. переглянути. Номер 2013. 13. URL: http://nbuv. gov.ua/j-pdf/tppd 2013 13 12.pdf (дата заявка: 9.11.2023).

51. Ковтун С. В. Інформаційна безпека : навч. Харків. Переглянути. ун-т, 2009. 368 с.

52. Корженьовський Л. Менеджмент безпеки. *Актуальні економічні*

проблеми. 2004. № 1 (31). З. 147-154.

53. Конституція України, Закон від 28.06.1996 р. No 254к/96-ВР. Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96- %D0%B2%D1%80 .

54. Корейський Н. Г. Формування сучасної інформаційної системи управління. Охорона військової частини : автореф. 2020. URL: http://ir.stu.cn.ua/123456789/19964 (дата звернення: 9.11.2023).

55. бакалавра мистецтв Організаційно-правові основи політики інформаційної безпеки в Україні: Монографія. Одеса: Юридична література, 2003. 472 с.

56. Бакалавр мистецтв Організаційно-правові основи політики інформаційної безпеки в Україні. Дисертація. ... доктор юридичних наук. наук: 12.00.07. Одеса. 2004. 427 с.

57. Котляров В. Основні підходи в концепції інформаційної безпеки. *Актуальні проблеми сучасної науки.* 2023. № 1(7). URL: https://doi.org/10.52058/2786-6300-2023-1(7)-474-484 (дата звернення: 9.11.2023).

58. Котляров В. Проблеми інформаційної боротьби в контексті забезпечення національні інтереси. *Наукові інновації та передові технології.* 2023. № 1(15). URL: https://doi.org/10.52058/2786-5274-2023-1(15)-499-511 (дата звернення: 9.11.2023).

59. Котляров В. Теоретичні основи сутності та поняття інформаційної безпеки. *Наукові перспективи (Наукові перспективи)* . 2023. № 6(36). URL: https://doi.org/10.52058/2708-7530-2023-6(36)-131-142 (дата звернення: 9.11.2023).

60. Кохановська О. В. Інформаційно-правові основи цивільно-правової відповідальності суспільства. *Право України,* 2015. № 4. С. 35-42.

61. Криволап Є., Юринець Ю. Взаємозв'язок стратегій безпеки України з інформаційною та кібербезпекою. *Актуальні проблеми сучасної*

науки. 2023. № 8(14). URL: https://doi.org/10.52058/2786-6300-2023-8(14)- 477-487 (дата звернення: 9.11.2023).

62. Кримінальний кодекс України. *Інформація Верховної Ради України (ВВР).* 2001, № 25-26, стор. 131. URL:https://zakon.rada.gov.Ua/laws/show/2341-14#Текст (дата звернення: 9.11.2023).

63. Крупнова А. ЕН. Перспективи правового регулювання інформаційної безпеки в Україні. *Актуальні проблеми боротьби з корупцією в Україні в умовах воєнного стану.* 2023. URL: https://doi.org/10.36059/978-966-397- 293-0-16 (дата звернення: 9.11.2023).

64. Кукляк Р. Роль і місце інформаційної безпеки в забезпеченні національної безпеки України. *Актуальні проблеми сучасної науки.* 2023. № 10(16). URL: https://doi.org/10.52058/2786-6300-2023-10(16)-227-239 (дата звернення: 9.11.2023).

65. Кульчій О. ЕН. Правове регулювання державної політики у сфері ЗМІ в Україні. *Юридичний форум.* 2015. № 3. С. 131-134.

66. Кустовська О. ЕН. Методологія системного підходу та наукових досліджень: Курс лекцій. Тернопіль: Економічна думка, 2005. 124 с.

67. Лазарєв В. Концептуальні основи державного управління інформаційною безпекою електронних послуг: теорія та проблеми. *Наукові перспективи.* 2023. № 6(36). URL: https://doi.org/10.52058/2708- 7530-2023-6(36)-143-150 (дата звернення: 9.11.2023).

68. Левківська В. М. Адміністративно-правове забезпечення на національному рівні безпеки. *Київський юридичний огляд.* 2023. № 4. Сторінка 83-88.URL: https://doi.org/10.32782/klj/2022.4.12 (дата звернення: 9.11.2023).

69. Леоненко Н.Ю. Зарубіжний досвід правового регулювання гарантій національна безпека. *Вісник Національного університету цивільного захисту України. серія: державне управління.* 2023. № 1(18)2023. URL: https://doi.org/10.52363/2414-5866-2023-1-14 (дата звернення: 9.11.2023).

70. Литовченко І. Є.Н. Основні тенденції інституалізації

інформаційно-комунікаційного середовища сучасного суспільства. *Вісник національного авіаційного університету. Середа. Соціологія. Політологія* : зб. наук. працює. Київ: НАУ, вип.2014. 1. С. 30-34.

71. Лийова С. Я., Пацелія Г. Ю. Спільна діяльність у сфері інформаційної безпеки. *Права людини та державне управління в сучасних умовах.* 2023. URL: https://doi.org/10.36059/978-966-397-314-2-78 (дата звернення: 9.11.2023).

72. Ліпкан В. А. Національна безпека України: Підручник. Київ: КНТ. 2009. 576 стор. URL: http://politics.enib.org.ua/pages-8286.html (дата звернення: 9.11.2023).

73. Ліпкан В.А., Максименко Ю. Є., Желіховський В.М. Інформаційна безпека України в контексті євроінтеграції: навч. Київ: КНТ, 2006. 280 с.

74. Лук'янченко О. ЕН. Господарське та організаційне забезпечення розвитку. Сектор комунального господарства міста. Донецьк, 2008 367 с.

75. Луцький М. Медіаграмотність як фактор комп'ютерної безпеки в Україні. *Наукові праці Національного авіаційного університету. Серія: Юридичний журнал « Авіаційне та космічне право».* 2023. Том 1, № 66. Сторінка 206-213.URL: https://doi.org/10.18372/2307-9061.66.17438 (дата звернення: 9.11.2023).

76. Ліанна Ю. IN. Визначення видів реабілітації у професійній підготовці майбутніх магістрів фізичної реабілітації. Вісник Чернігівського національного педагогічного університету. Сер.: Педагогічні науки. Фізкультура і спорт. Номер 2013. 112(2). З. 177-182.

77. Ляхович Г. Й. Про сучасне розуміння сутності та особливостей державного управління в державі. *Вісник ХНУВС.* 2009. № 3 (46). З. 129 136.

78. Магула М. Феномен комп'ютерного тероризму як загроза національній безпеці та міжнародна безпека.03.07.2014.URL: https://naub.oa.edu.ua/2014/phenomenon-informatics-teroryzmu-yak- національні та міжнародні загрози/ (дата звернення: 08.07.2019).

79. Марта В. П., Усата Г. ЕН. Інформаційно-аналітичне забезпечення. Діяльність поліції як складова частина системи заходів щодо забезпечення безпеки державної інформації. *Морська безпека та оборона.* 2023. № 1. С. 62-68. URL: https://doi.org/10.32782/msd/2023.L8 (дата звернення: 9.11.2023).

80. Малик Я. Ю., Береза О. Ю. Забезпечення інформаційної безпеки України в контексті світового досвіду. *Ефективність державного управління.* Номер 2012. 32. С. 20-27.

81. Мамонов І. Потреби та інтереси людини як основа державного управління. *Вісник Національної академії державного управління при Президентові України.* Число 2012. 3. С. 212-220.

82. Марков О. О. Постправда та фактчекінг – тренди сучасної комунікації. *Наука і освіта: ключові проблеми сучасності.* 2018.Т11. Сторінка 11-119.

83. Марущак А. І. Дослідження проблем інформаційної безпеки в юридичних науках. *Правова інформатика.* 2010. № 3(27). З. 17-21.

84. Ведмідь В. Ю., Правдивець О. М., Кривчун Р. Ю. Теоретико-метод Принципи формування системи управління інформаційною безпекою підприємства. *Агросвіт.* 2023.№ 1.С. 24-30.URL: https://doi.org/10.32702/2306-6792.2023.L24 (дата звернення: 9.11.2023).

85. Мельничук О. Є.Н. Правові механізми управління критичною інформаційною інфраструктурою України. *Збірник наукових праць Національної академії державного управління при Президентові України.* 2018. № 1. С. 42-60. URL: https://doi.org/10.36030/2664-3618- 42-1-2018 (дата звернення: 9.11.2023).

86. Мокій А. ЕН. Дослідження методів управління ризиками в системах управління Інформаційна безпека. 2018. 99 с. URL: https://ela.kpi.ua/handle/123456789/26820 (дата звернення: 9.11.2023).

87. Мохова Ю. Л., Луцька А. Й. Сутність та основні напрями державної інформаційної політики України. *Державне управління: вдосконалення та розвиток* : ел. наук. професія. переглянути. / Дніпропетровськ. економіко-

аграрного статусу ВНЗ 2018. № 12. URL: http://www.dy.nayka.com.ua/pdf/122018/27.pdf (дата звернення: 9.11.2023).

88. Мохор В., Цуркан В. Методика побудови систем управління інформаційною безпекою. *Український журнал досліджень інформаційної безпеки.* 2022. Том 23, № 4. Стор. 200-211. URL: https://doi.org/10.18372/2410-7840.23.16766 (дата звернення: 9.11.2023).

89. ю. Є. Муравська (Якубівська) Інформаційна безпека суспільства: концептуальний аналіз. *Економіка і суспільство.* Номер 2017. № 9. С. 289-294 .

90. Наконечний В. КОН. Стан розвитку управління інформаційною безпекою у світовій практиці та його вплив на економічний розвиток України. *Сучасний захист інформації.* 2015. № 4. С. 10-15.

91. Настюк В.Я., Бєлєвцева В.В. Правовий захист прав на інформацію та Свободи людини в Україні: проблеми та перспективи Інформація і право. № 2(14).2015.URL: http://ippi.org.ua/sites/default/files/nvybvvpzips_14_2_2015.pdf (дата заявка: 9.11.2023).

92. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

Масова комунікація: принципи та механізми на основі узагальнення світового досвіду. *Державне управління: теорія і практика* : ел. наук. професія. переглянути. 2011. № 2. URL: http://academia. gov.ua/ej/ej 14/txts/Nesteryak.pdf (дата звернення: 9.11.2023) .

93. Норчук Ю. IN. Правові аспекти інформаційної безпеки в Україні. Сучасна війна: гуманітарний аспект. 2017. URL: http://www.hups.mil.gov . ua/assets/doc/science/stud-conf/suchasna-viyna-gumanitamiy-aspekt/26 .pdf (дата звернення: 9.11.2023).

94. Овчаренко М. Центр оперативного управління інформаційною безпекою. *Передові відкриття сучасної науки: досвід, підходи та інновації* / Кафедра О. Северінова. 2021. URL: https://doi.org/10.36074/logos-09.04.2021.v1.49 (дата звернення: 9.11.2023).

95. Овчаренко М. Ю., Северинов О. Е. Н. Аналіз кореляційних правил у системах захисту інформації та управління подіями безпеки: автореф. 2021. URL: https://openarchive.nure.ua/handle/document/15763 (дата звернення: 9.11.2023) .

96. Овчаренко М. Ю., Северинов О. Е. Н. Аналіз сучасних систем менеджменту

Інформаційна безпека та інциденти безпеки: автореф. 2019. URL: https://openarchive.nure.ua/handle/document/15774 (дата звернення: 9.11.2023) .

97. Оліян О. ЕН. Адміністративні реформи та їх вплив на забезпечення інформаційної безпеки в Україні. *Наукові записки Інституту законодавства Верховної Ради України.* 2012. № 4. С. 53-56.

98. Оліян О. ЕН. Адміністративно-правові основи інформаційної безпеки. *Європейські перспективи.* 2012. № 4(1). З. 65-68.

100.Олійник О. Є.Н. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки в Україні. *Наукові записки Інституту законодавства Верховної Ради України.* 2015. № 1. С. 54-59. Інформаційна

безпека та її складова: захист інформаційних ресурсів. *Закон і безпека.* 2014. № 1 (52). З. 103-108.

101. Олійник О. В. Методологічні засади забезпечення системи

102.Олійник О. Є.Н. Правові аспекти оптимізації організаційних засад інформаційної безпеки. *Бюлетень Міністерства юстиції України.* 2013. № 1 (135). З. 73-78.

103.Олійник О. Є.Н. Принципи забезпечення інформаційної безпеки в Україні. *Наукові праці Національного авіаційного університету. Юридичний вісник «Авіаційне та космічне право».* 2016. № 4 (41). З. 72-78.

104. Опанасенко Я . IN. Роль і місце організаційної, соціальної та інформаційної складових у реалізації державної регіональної політики в умовах регіональної невизначеності. *Вісник Національного університету цивільного захисту України (Серія: Державне управління справами),* 2016. No 1 (4). З. 203-209.

105.Опірський І. Р., Головчак Р. В., Мосійчук І. А. Перспективи розвитку систем штучного інтелекту в контексті забезпечення інформаційної безпеки. *Український науковий журнал з інформаційної безпеки.* 2023. Том 26, № 2. Стор. 108-115. URL: https://doi.org/10.18372/2225-5036.26.14965 (дата звернення: 9.11.2023).

106. Острякова В. ю. Формування системи управління інформаційною безпекою підприємства : тези.2017.URL:

https://er.knutd.edu.ua/handle/123456789/8187 (дата звернення: 9.11.2023).

107. Панченко О. Турбулентні соціально-психологічні виклики в системі

Управління державною інформаційною безпекою. *Теорія і практика державного управління.* 2020. Том 1, № 68. Сторінка 210-217.URL:

https://doi.org/10.34213/tp.20.01.25 (дата звернення: 9.11.2023).

108. Панченко О. А., Сердюк І. Ю. Роль держави в особистих і суспільних відносинах у бурхливий час. Матеріали Міжнародної науково-

практичної Інтернет-конференції *«Тенденції та перспективи розвитку науки та освіти в умовах глобалізації». (28.02.2020)* Переяслав - 2020. Освіта вища. 56. С. 42-45.

109. Пічура В. ю. Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів: дис. 2021. URL: http://elar.khnu.km.ua/jspui/handle/123456789/10388 (дата звернення: 9.11.2023).

110. Довідково: Закон України від 02.10.1992 № 2658-XII [Редакційна редакція від 03.12.2019]. Сайт Верховної Ради України. URL: https://zakon.rada . gov.ua/laws/show/2657-12 (дата звернення: 9.11.2023).

111. Про концепцію Національної програми інформатизації: Закон України;

Концепція від 04.02.1998 № 75/98-ВР.URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80

112. Про національну безпеку України: Закон України від 21.06.2018 № 2469 - VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19

113. Про Національну програму інформатизації: Закон України від 04.02.

1998 р. No 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

114. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 01.09.2007 р. № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16ffТекст

115. Про Службу безпеки України: Закон України від 25 березня 1992 р. Відомості Верховної Ради. 1992. № 27. ст. 382.

116. Про Службу зовнішньої розвідки України: Закон України від 01.12.2005 р. № 3160. Відомості Верховної Ради України. 2006. № 8. Ст.231. 94.

117. Про судоустрій і статус суддів: Закон України від 26.04.01. № 2402-III. URL: https://zakon.rada.gov.ua/laws/show/1402-19ffText (Редакційна версія від 20.06.2020) (дата звернення: 09.11.2023)

118. Редзюк В., Редзюк Н. Сучасні проблеми інформаційної безпеки в

Україні

та напрямки її вирішення. *Публічне управління: поняття, парадигма, розвиток, удосконалення.* 2023. № 3. Сторінка 59-65.URL: https://doi.org/10.31470/2786-6246-2023-3-59-65 (дата звернення: 9.11.2023) .

119. Терещенко О. Правові аспекти забезпечення національної безпеки в Україні. *Міжнародна та національна безпека: теоретичні та прикладні аспекти.* 2023. URL: https://doi.org/10.31733/17-03-2023-98-99 (дата звернення: 9.11.2023).

120. Тимошенко Ю., Кисленко Д. Поліція охорони Національної поліції України як суб'єкт забезпечення інформаційної безпеки в умовах воєнного стану. *Наукові праці Міжрегіональної академії управління персоналом. Юридичні науки.* 2023. № 1 (63). З. 53-59. URL: https://doi.org/10.32689/2522-4603.2023.1.8 (дата звернення: 9.11.2023).

121. Філіпішина Л., Костик Є., Дзевелюк М. Публічне управління у сфері інформаційної безпеки (подолання сучасних загроз). *Актуальні проблеми сучасної науки.* 2023. № 5(11). URL: https://doi.org/10.52058/2786-6300- 2023-5(11)-196-205 (дата звернення: 9.11.2023).

122.Чубаєвський В. Методи управління корпоративною інформаційною безпекою. *Економіка і суспільство.* 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-49 (дата звернення: 9.11.2023).

123. Шабуніна В., Тур О. Медіаграмотність як ключовий фактор

Безпека інформації фізичної особи. *VH Міжнародна науково-практична конференція «Психолого-педагогічні, правові та соціокультурні проблеми сучасного суспільства».* 2023. URL: https://doi.org/10.32782/fphisn.2023.1.42-43 (дата звернення: 9.11.2023).

124. Шевченко А.Є., Француз А.Ю., Кудін С. Е.Н. Методологічні принципи

Нормативно-правове забезпечення інформаційної безпеки. *Ірпінський*

юридичний журнал. 2023. № 2(11). З. 48-55.URL: https://doi.org/10.33244/2617-4154-2(11)-2023-48-55 (дата звернення: 9.11.2023) .

125. Шевченко В. і. Передовий світовий досвід управління інформаційною безпекою та його вплив на економічну стабільність держави. *Сучасний захист інформації.* 2015. № 4. С. 4-9.

126. Шинкар Т., Левченко Т., Дудар В. Маніпулятивні технології в аспекті інформаційної безпеки. *Комунікаційний документ компанії.* 2023. № 19. З. 270-286. URL: https://doi.org/10.31470/2518-7600-2023-19-270-286 (дата звернення: 9.11.2023).

127. Шульга О. Ю. Рекламно-інформаційний менеджмент компаній. *Підприємництво і комерція.* 2023. № 38. С. 84-93. URL: https://doi.org/10.32782/2522-1256-2023-38-11 (дата звернення: 9.11.2023).

128. Архипов О., Теплицька Т. Адаптивний підхід до інформаційної безпеки управління. *Молодий вчений.* 2019. Т. 11, №. 75. URL: https://doi.org/10.32839/2304-5809/2019-11-75-142 (дата звернення: 9.11.2023) .

129. Брацук І., Кавин С. Міжнародно-правове регулювання забезпечення інформаційної безпеки безпеки в рамках ООН. *Вісник Київського національного університету імені Тараса Шевченка. правознавство.* 2023. № 125. С. 21-26. URL: https://doi.org/10.17721/1728-2195/2023/L125-4 (дата звернення: 09.11.2023).

130. Несен М., Ляшевська В., Фоміна Ю. Управління інформаційною безпекою виробництва. *Економіка: часові реалії.* 2021. Т. 2, № 54. С. 39-46. URL: https://doi.org/10.15276/etr.02.202L5 (дата звернення: 17.12.2023).