Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра публічного управління, адміністрування та права

Кваліфікаційна робота

на тему: **«ПУБЛІЧНЕ УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД КРАЇН ЄС ДЛЯ УКРАЇНИ»**

Виконав:
студент академічної групи 2м – ДС
освітньо-професійної програми
«Публічне управління та адміністрування»
другого (магістерського) рівня вищої освіти
спеціальності 281
«Публічне управління та адміністрування»
Число А.В.
Науковий керівник:
завідувач кафедри публічного управління,
адміністрування та права, кандидат наук з
державного управління, доцент
Кульчій І.О.

Полтава – 2023 рік

ЗМІСТ

ВСТУП

Актуальність. Останнім часом проблема забезпечення національної безпеки зміщується в бік не стільки декларованої, скільки фактично розглянутої. Насамперед, це пов’язано з посиленням зовнішніх загроз безпечному розвитку України: посиленням мілітаризації держав регіону, використанням позиції енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї та так далі.

Із зростанням значення інформації в суспільному житті як ресурсу розвитку, з посиленням глобальних впливів на нації та держави актуальним стає проблема збереження та постійного оновлення їх національного інформаційного простору. Під час інформаційної агресії вона є об’єктом первинного ураження та суб’єктом організації захисту сторони, яка зазнала інформаційної агресії.

Сучасний національний інформаційний простір як сфера інформаційного обміну має складатися з розгалуженої системи структур, що забезпечують створення нової інформації, зберігання та захист існуючої, а також організацію її використання через мережу засобів у країні та за кордоном для задоволення інформаційних інтересів і потреб громадян і зрештою - інформаційна безпека держави.

Проблема інформаційної безпеки Європейського Союзу розглядається поряд з іншими проблемами інформаційного суспільства. Слід зазначити, що аналіз низки нормативно-правових актів та планів дій у сфері формування інформаційного суспільства ЄС дозволив зробити висновок про значно вужче розуміння поняття «інформаційна безпека» стосовно як до України, так і до України. міжнародне право.

Реформування сфери державного управління забезпечення інформаційної безпеки не є виключенням і передбачає проведення ґрунтовної роботи щодо адаптації національної системи адміністрування забезпечення

інформаційної безпеки у відповідності з кращими практиками держав Європейського Союзу. Відповідно, актуальним є науково-практичне завдання щодо узагальнення досвіду забезпечення інформаційної безпеки у розвинених державах світу і, зокрема деяких країн, що входять до Європейського Союзу та США.

Дослідженням проблем займались такі вітчизняні та зарубіжні вчені: 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.

Мета магістерської роботи полягає в аналізі публічного управління забезпеченням інформаційної безпеки в країнах Європейського союзу, США та використання їхнього досвіду для вдосконалення інформаційної безпеки України.

Для досягнення поставленої мети були визначені такі **завдання**:

- розкрити поняття, сутність, історію виникнення проблеми забезпечення інформаційної безпеки;
- охарактеризувати принципи забезпечення інформаційної безпеки;
- проаналізувати нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині;
- здійснити аналіз забезпечення інформаційної безпеки в органах публічної влади в США;
- визначити напрями вдосконалення забезпечення інформаційної безпеки через адаптацію кращого зарубіжного досвіду та удосконалення організації доступу до публічної інформації.

Об’єкт дослідження - суспільні відносини, що склалися в процесі публічного управління забезпеченням інформаційної безпеки в Європейському Союзі та Сполучених Штатах Америки.

Предметом дослідження є досвід публічного управління в окремих країнах ЄС та США із забезпечення інформаційної безпеки.

Практичне значення дослідження може бути використане у науково-дослідній сфері, у правотворчій діяльності, у правовиховній роботі, у навчальному процесі.

Наукова новизна дослідження полягає у теоретичному обґрунтуванні та практичному вирішенні комплексу питань, пов'язаних із публічним управлінням забезпечення інформаційної безпеки в Україні із використанням досвіду країн ЄС та США.

У процесі написання даної магістерської використано сукупність загальнонаукових **методів**: метод аналізу наукових праць, метод аналізу, метод порівняння, а також – поєднання історичного та логічного методів, і міждисциплінарного підходу з використанням даних історії, політології, права та інших дисциплін.

Інформаційну основу дослідження складають бази нормативних документів, статистичні та спеціальні періодичні довідники, вітчизняні й закордонні видання, збірники наукових праць з теми роботи.

Структура роботи. Магістерська робота складається зі вступу, трьох розділів, висновків та списку використаних джерел.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття, сутність, історія виникнення проблеми забезпеченням інформаційної безпеки

Характеризуючи поняття, сутність, історія виникнення проблеми забезпеченням інформаційної безпеки, варто зауважити, що у Радянському Союзі питання інформаційної безпеки та захищеності інформаційного простору було «покладено на Державну комісію СРСР з питань протидії іноземним технічним розвідкам, створену в 1973 р. За період існування Комісії було створено потужну систему органів захисту інформації та забезпечення ІБ» [31].

8 грудня 1991 р. було «підписано Угоду про створення СНД. 21 грудня 1991 р. голови одинадцяти незалежних держав колишніх республік СРСР підписали Протокол про утворення СНД та прийняли Алма-Атинську Декларацію» [31].

Грузія приєдналась до СНД двома роками пізніше та остаточно вийшла зі складу Співдружності у 2010 через російсько-грузинську війну 2008 р. 22 січня 1993 р. Радою голів держав «було прийнято Статут СНД, який є чинним у теперішній час. Україна має статус держави-засновника СНД, проте Статут СНД не підписала».

Відповідно до Угоди та Статуту метою Співдружності є розвиток рівноправного та взаємовигідного співробітництва у багатьох сферах, сприяння широкому обміну інформацією та дотримання взаємних зобов’язань.

Лише 18 жовтня 1996 року, майже через п’ять років після заснування Співдружності, «була прийнята Концепція формування інформаційного простору СНД. У ній, зокрема, було визначено завдання щодо забезпечення

кожною з держав-учасниць Співдружності власної інформаційної безпеки та, відповідно, захист інформаційного суверенітету. З цією метою держави-учасниці зобов'язувались проводити своєчасний моніторинг загроз в інформаційній сфері та вдосконалювати інформаційну політику» [31].

На жаль, у тодішньому варіанті Концепції«не було відображено питання підготовки й проведення інформаційних війн та інформаційно-психологічних операцій. Таким чином, одне з головних питань у сфері інформаційної безпеки на багато років опинилось поза сферою правового врегулювання» [31].

Рішенням Ради голів урядів СНД від 25 листопада 1998 р. був затверджений «Перспективний план підготовки документів і заходів з реалізації Концепції» щодо «формування інформаційного простору СНД, а у наступному 1999 р., було затверджено Концепцію інформаційної безпеки держав-учасниць СНД у військовій сфері, яку підписали Республіки Вірменія, Білорусь, Казахстан, Киргизська, Російська Федерація та Таджикістан, тобто держави-учасниці ОДКБ».

Відповідно до Концепції визначено джерела загроз інформаційній безпеці у військовій сфері: «державна політика зарубіжних країн, спрямована на моніторинг політичних, економічних, військових, екологічних та інших процесів з метою отримання односторонніх переваг; відсутність єдиної політики, інфраструктури та необхідної нормативно-правової бази в інформаційній сфері» [31].

10 жовтня 2008 р. у м. Бішкек Рішенням Ради голів держав СНД було затверджено Концепцію співробітництва держав-учасниць СНД у сфері гарантування інформаційної безпеки. Зазначені документи підписали тільки держави-учасниці ОДКБ» [31].

Наступними документами у сфері інформаційної безпеки держав-учасниць Співдружності стала Стратегія співробітництва держав-учасниць СНД щодо побудови та розвитку інформаційного суспільства, «затверджена 28 вересня 2012 р. та План дій щодо її реалізації на період до 2015 року, а

також Модельний інформаційний кодекс для країн-учасників СНД. Їхню розробку здійснювала базова організація держав-учасниць СНД з методичного та організаційно-технічного забезпечення робіт у галузі інформаційної безпеки та підготовки фахівців у цій сфері. Рішенням Ради голів урядів СНД від 30 травня 2012 р. статус Базової організації було надано федеральному державному унітарному підприємству» [37].

Відповідно до Рішення РНБО України від 23 квітня 2008 р. № 377/2008 Кабінету Міністрів України було доручено затвердити «Доктрину інформаційної безпеки України», «Державну програму формування позитивного іміджу України та перелік заходів щодо розширення фінансової підтримки культурно-інформаційних центрів при дипломатичних установах України», передбачити розширення таких центрів (Рішення скасовано на підставі рішення РНБО України n0008525-14 від 28 квітня 2014 р.). Указом Президента за №514/2009 було затверджено «Доктрину інформаційної безпеки України» (Указ втратив чинність на підставі Указу Президента України №504/2014 від 06 червня 2014 р.).

Щодо характеристики сутності самого поняття інформаційна безпека, варто зауважити, що «інформаційна безпека – це такий стан при якому людина спроможна, до уникнення спрямованого, в першу чергу – неусвідомленого поганого впливу інформації» [6, с. 78].

Таблиця 1.1. Характеристика концепції «інформаційної безпеки» за твердженнями різних науковців

Автор	**Особливості концепції**
РА Балта	«Інформаційна безпека - це вид правовідносин публічної інформації про створення, підтримку, та захист безпечних умов життя, бажаних для людини, суспільства та держави; публічно-правові відносини, пов'язані зі створенням, розповсюдженням, зберіганням та використанням інформації»
Б.А. Волан	«Інформаційна безпека - це стан захисту встановлених законом норм та параметрів процесів та інформаційних відносин, які забезпечують необхідні умови для існування держави, людини та суспільства як суб'єктів цих процесів та відносин»
О.Л. Морозов	«Державна інформаційна безпека – це стан державних

	інститутів та суспільства, що забезпечує надійний захист національних інтересів країни та її громадян в інформаційній сфері»
В.А. Ліпіціос	«Інформаційна безпека – це складова національної безпеки, процесу управління загрозами та небезпеками державних та недержавних інститутів, окремих громадян, що забезпечує інформаційний суверенітет України»
Н.Р. Нижній, Г.П. Ситник, В. Т. Білоус	«Поняття інформаційної безпеки визначено на основі найімовірніших загроз національній безпеці України у життєво важливих сферах. Зокрема, в галузі інформаційної безпеки вчені розуміють стан правових норм та пов'язаних із ними інститутів безпеки, які гарантують постійну доступність даних для прийняття стратегічних рішень та захисту інформаційних ресурсів країни.

Примітка: власна розробка автора

Але наскільки це запропоноване визначення відповідає своїй суті та відповідає суті поняття «інформаційний простір», ми намагатимемося розібратися докладніше.

Щоб зрозуміти напрямок розглянутого простору, необхідно згадати, що мається на увазі під поняттям «кібернетика», похідним якого є «кібернетика». Кібернетика - «наука про управління, комунікацію та обробку інформації. Основний об'єкт дослідження - звані кібернетичні системи, аналізовані абстрактно, незалежно від своїх матеріальної природи. Приклади кіберсистем - автоматичні регулятори у технологіях, комп'ютерах, людському мозку, біологічних популяціях, людському суспільстві. Кожна така система є набором взаємопов'язаних об'єктів (елементів системи), які здатні сприймати, запам'ятовувати та обробляти інформацію, а також змінювати її». [23. С. 456.].

З вищевикладеного можна дійти невтішного висновку, що «інформаційний простір - це форма співіснування сукупності матеріальних і нематеріальних об'єктів і процесів, вкладених у формування, сприйняття, запам'ятовування, обробку та обмін інформацією».

Інформаційний простір має такі властивості:

- «довжина»;
- «Єдність розсуду та наступності»;

– «Істотність та нематеріальність»;
– «Абстракція та реальність»;
– «Реальність загального впливу» [28, с. 314.].

Рисунок 1.1 Властивості інформаційного простору

Примітка: побудовано автором на підставі джерела [28]

Інформаційний простір має розмір/довжину, який визначається кількістю матеріальних та нематеріальних об'єктів, доступних протягом певного періоду часу. У той час як довжина кіберпростору обмежена поверхнею земної кулі з точки зору матеріальних об'єктів, довжина інформаційного простору практично необмежена з точки зору присутності нематеріальних об'єктів.

Інформаційний простір включає у собі як матеріальну складову, наприклад, комп'ютерне устаткування, засоби зв'язку, матеріальні компоненти телекомунікаційних мереж, алгоритми записи і коди тощо. буд., і нематеріальне - інформацію, процеси читання коду, процеси передачі і т. буд. Але слід зазначити, що під матеріальністю в цьому випадку ми маємо на увазі, на відміну від філософського розуміння, все, що можна побачити, відчути або помацати.

Таким чином, інформаційний простір - це рукотворний продукт людини, який вона сформувала для себе і для задоволення своїх потреб, не замислюючись про «бічні» явища, про які буде сказано нижче.

Це і сказане вище дає підстави стверджувати, що:

- «об'єктами інформаційного простору є живі істоти та їхні групи, здатні сприймати, запам'ятовувати та обробляти інформацію та змінювати її, включаючи, насамперед, людину, певні сегменти суспільства та суспільства в цілому, державу; , природні та штучні інформаційні відносини між ними та їх формування та використання, а також матеріальні та нематеріальні об'єкти та процеси, спрямовані на створення, сприйняття, запам'ятовування, зберігання, обробку та обмін інформацією»;

- «Суб'єктами кіберпростору є людина, суспільство, держава і жива істота, яка здатна сприймати, запам'ятовувати та обробляти інформацію, а також змінювати її» [28, с. 315.].

Але подальші дослідження визначення «інформаційної безпеки» мають виявити відмінності в поняттях «інформаційний простір» та «кіберпростір».

Інформаційний простір - це «форма співіснування сукупності матеріальних і нематеріальних об'єктів і процесів, вкладених у задоволення інформаційних потреб всіх живих істот Землі» [28, стор 315].

Інформаційний простір - це «форма співіснування безлічі матеріальних і нематеріальних об'єктів і процесів, вкладених у задоволення інформаційних потреб всіх живих істот Землі».

Насамперед, слід розуміти, що згідно з цим визначенням інформаційна безпека – це «стан систем, який нейтралізує загрози доступності, цілісності чи конфіденційності даних, що циркулюють в інформаційних системах. Крім того, у зв'язку з включенням до списку об'єктів, які можуть бути порушені кіберзагрозами комп'ютерних сервісів, визначення терміна передбачає наявність загроз функціональності систем вищого порядку, до яких відносяться інформаційні системи. Це положення має важливий

методологічний зміст для розуміння місця та ролі проблеми інформаційної безпеки в інших типах безпеки» [28, с. 316.].

У німецькій стратегії «інформаційна безпека означає комплекс необхідних та адекватних заходів, реалізація яких мінімізує ризики. При цьому у стратегії йдеться, що інформаційна безпека має ґрунтуватися на комплексному підході. Це досить прагматична точка зору, яка дозволяє розробити практичні кроки щодо забезпечення інформаційної безпеки, але не забезпечує достатньої методологічної основи для проектування та оцінки систем, які забезпечують цю безпеку. Про це свідчить зміст десяти стратегічних напрямів у стратегії інформаційної безпеки, оголошеної федеральним урядом Німеччини» [28].

«У Канаді стверджують, що для забезпечення найбільш актуального використання інформаційного простору, який є стратегічним активом, необхідно передбачати кіберзагрози і протидіяти їм. Стратегія інформаційної безпеки Канади не дає чіткого визначення, що таке інформаційна безпека. Згідно з цим документом, інформаційна безпека може розумітись як захист кіберсистем від шкідливого неправомірного використання та інших деструктивних атак. З іншого боку, дається докладне визначення кібератаки, і кібербезпека є засобом захисту від цих загроз». [42].

В цілому, канадська стратегія, як і раніше, спрямована на усунення основної шкоди при реалізації кіберзагроз, наприклад, збитків, які можуть завдати системи життєзабезпечення, та підтримки діяльності всієї країни, бізнесу та людей.

Одна з останніх національних стратегій інформаційної безпеки (Турецька Республіка) містить таке визначення: інформаційна безпека – «захист інформаційних систем, що є частиною інформаційного простору, від атак, забезпечення конфіденційності, цілісності та доступності інформації, що обробляється в цьому просторі, виявлення та реагування на атаки та кіберінциденти. Кіберпростір означає середовище інформаційних систем, розподілених у всьому світі, включаючи мережі, що з'єднують ці системи.

Національний кіберпростір визначається як простір, що складається з інформаційних систем суб'єктів, що перебувають під юрисдикцією Турецької Республіки» [60].

«Нідерланди також приділяють особливу увагу загрозі інформаційній інфраструктурі у контексті загального використання цифрових технологій (комп'ютерів). У 2013 році Національний координатор з безпеки та боротьби з тероризмом опублікував Національну стратегію інформаційної безпеки. На думку авторів стратегії, інформаційна безпека - це комплекс зусиль щодо запобігання збиткам, які можуть бути заподіяні збоями у функціонуванні ІКТ або їх неправильним використанням, а також відновлення ІКТ після реалізації цих загроз» [33].

Однак у цій стратегії було зроблено дуже важливий методологічний висновок – інформаційна безпека може бути досягнута лише у систематичному взаємозв'язку з вирішенням проблем захисту та захисту основних прав, цінностей та соціально-економічних благ суспільства.

Метою політики уряду Австралії в галузі інформаційної безпеки є «підтримка безпечної, стійкої та надійної роботи електронного операційного середовища, яке підтримує національну безпеку Австралії та максимізує переваги цифрової економіки. Стратегія інформаційної безпеки, опублікована у 2009 році, спрямована на забезпечення доступності, цілісності та конфіденційності ІКТ в Австралії, а також на захист людей, особливо дітей, від наслідків незаконного та образливого контенту, кіберзалякування, переслідувань та використання ІКТ» [49].

В українському законопроекті представлена власна версія визначення інформаційної безпеки, що означає «стан захисту життєво важливих інтересів людини та громадянина, суспільства та держави у кіберпросторі». Таким чином, «у кіберпросторі - середовище, що виникає в результаті роботи на основі єдиних принципів та за загальними правилами інформаційних систем, телекомунікацій та інформаційно-телекомунікаційних систем. Це визначення має дуже низький методологічний потенціал і дозволяє

специфікувати функції захисту. Більше того, проблеми функціонування інформаційних систем у загальному сенсі абсолютно необґрунтовані, в результаті телебачення та радіо, а також бібліотеки та архіви можуть бути віднесені до проблем інформаційної безпеки» [3].

Враховуючи, що проблема інформаційної безпеки має глобальний характер, позиція міжнародних організацій видається дуже цікавою. Таким чином, Міжнародний союз електрозв'язку визначає у своїй Рекомендації наступне: інформаційна безпека – «це набір інструментів, стратегій, принципів безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, навчання, практичного досвіду, страхування та технологій, які можна використати. для захисту інформаційного середовища, ресурсів організації та користувача» [28].

Ресурси організації та користувача включають «підключені обчислювальні пристрої, персонал, інфраструктуру, додатки, послуги, телекомунікаційні системи та всю інформацію, що передається та/або зберігається в інформаційному середовищі, і мета інформаційної безпеки полягає в тому, щоб спробувати досягти та підтримувати безпеку. властивостей ресурсів організації або користувача відповідних загроз інформаційної безпеки. Загальні цілі безпеки включають доступність, цілісність, яка може включати справжність та надійність, конфіденційність» [22, с. 24].

Проблема інформаційного менеджменту – це елемент національної безпеки, безпеки держави.

Виходячи з вищевикладеного, у роботі дано визначення, що «інформаційна безпека – стан людського потенціалу, суспільства та держави щодо запобігання та запобігання спрямованому, насамперед – неусвідомленому, негативному впливу (інформаційна) робота – інформаційна безпека. - стан захищеності важливих інтересів людини, суспільства та держави, що запобігає завданню шкоди» [42]:

– «Вплив негативної інформації, насамперед, шляхом створення, розповсюдження, несанкціонованого використання інформації, свідомо спрямованої для певної мети, неповної, несвоєчасної, небезпечної та упередженої»;

– «Негативні наслідки використання інформаційних технологій»;

– «Несанкціоноване порушення режиму доступу до інформації з її поширенням та подальшим використанням є правильним» [42].

У світі інформація - найцінніший глобальний ресурс. Економічний потенціал компанії багато в чому визначається кількістю інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація ускладнюється, якісно змінюється, зростає кількість її джерел та споживачів. Водночас зростає вразливість сучасного інформаційного суспільства перед небезпечною (а іноді й шкідливою) інформацією, її передчасним прийомом, промисловим шпигунством, кіберзлочинністю тощо. Тому Конституція України вважає інформаційну безпеку однією з найважливіших функцій держави [4].

Згідно з науковими дослідженнями, «Система захисту інформації в Україні не виконує деяких важливих функцій. Зокрема, управління його діяльністю неефективне, організаційні зміни, що вносяться до адміністративної реформи, мають безсистемний характер, проводяться без попереднього функціонального опрацювання органів державної влади. Негативні тенденції в національному інформаційному просторі, криза економіки країни та інші фактори визначають ескалацію загроз, які можуть призвести (а іноді й призвести) до значних втрат політичного, економічного, військового та іншого характеру, що завдає шкоди юридичним особам та громадянам» [8, с. 90].

Враховуючи вищезазначене, варто зосередити увагу на одному з найважливіших аспектів забезпечення адекватного захисту інформації - координації дій державних органів, приватного сектору, НУО та окремих осіб. Відповідно до статті 17 Конституції України забезпечення безпеки

інформації – «справа всього українського народу. Питання координації важливий саме собою і важливий оскільки, на відміну багатьох інших галузей, у сфері інформаційних технологій термінологія постійно змінюється, «ламаючи» традиційні ставлення до методи і засоби передачі, прийому, обробки і місце зберігання. Інформація. Хоча іноді зміна фіксованих термінів простежується лише у роботі маркетологів з просування своїх проектів.1].

«Проблема інформаційної безпеки може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформації. Концептуальними є пропозиції щодо широкого залучення вчених та вітчизняних виробників до її вирішення як складової національної безпеки. Внутрішні спеціалісти повинні гарантувати якісні інформаційні послуги, безпеку інформаційних технологій, сучасну систему сертифікації програмного та апаратного забезпечення, впровадження стандартизації, створення національних баз даних, телекомунікаційні системи, безпеку робочих місць у світовому інформаційному просторі» [2].

Ігнорування цих питань може призвести до труднощів при прийнятті важливих політичних, економічних, соціальних, військових рішень тощо.

«Рівень інформаційної безпеки активно впливає на політичну, економічну, оборонну та інші складові національної безпеки України, оскільки найчастіше реалізація інформаційних загроз є згубним завданням у політичній, військовій, економічній, соціальній, екологічній сферах. і так далі» [18, с. 129].

На жаль, сьогодні в Україні немає реальних гарантій безпеки її інформації, немає зведення нормативних документів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес комп'ютеризації носить стихійний, неконтрольований характер, з переважаючою тенденцією до використання засобів комп'ютеризації іноземного виробництва.

Отже, характеризуючи концепцію, сутність, історію проблеми інформаційної безпеки. слід зазначити, що за країнами СРСР, як і в Україні, розвиток напрямів досліджень інформаційної безпеки людини та суспільства загалом розпочався лише в останнє десятиліття XX століття. Це пов'язано з початком демократичних реформ, пов'язаних із встановленням незалежності та автономії держави. Інформаційна безпека – це стан захисту життєво важливих інтересів людини, суспільства та держави при використанні інформаційних систем та/або телекомунікаційних мереж. .. Неповнота, своєчасність та неточність використовуваної інформації; негативний вплив на інформацію; негативні наслідки експлуатації інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

1.2 Принципи управління забезпеченням інформаційної безпеки

Аналіз принципів інформаційної безпеки дозволяє стверджувати, що «вітчизняне право виробило необхідні теоретичні засади для вирішення проблеми обґрунтування узагальненої системи принципів організації та управління забезпеченням інформаційної безпеки. Тому питання подальшого детального визначення існуючих та обґрунтування нових, більш ефективних принципів, яке на даний час залишається, по суті, відкритим, за існуючим станом забезпечення інформаційної безпеки є вельми актуальним. Викладене свідчить про складність проблеми визначення методологічних засад управління забезпеченням інформаційної безпеки».

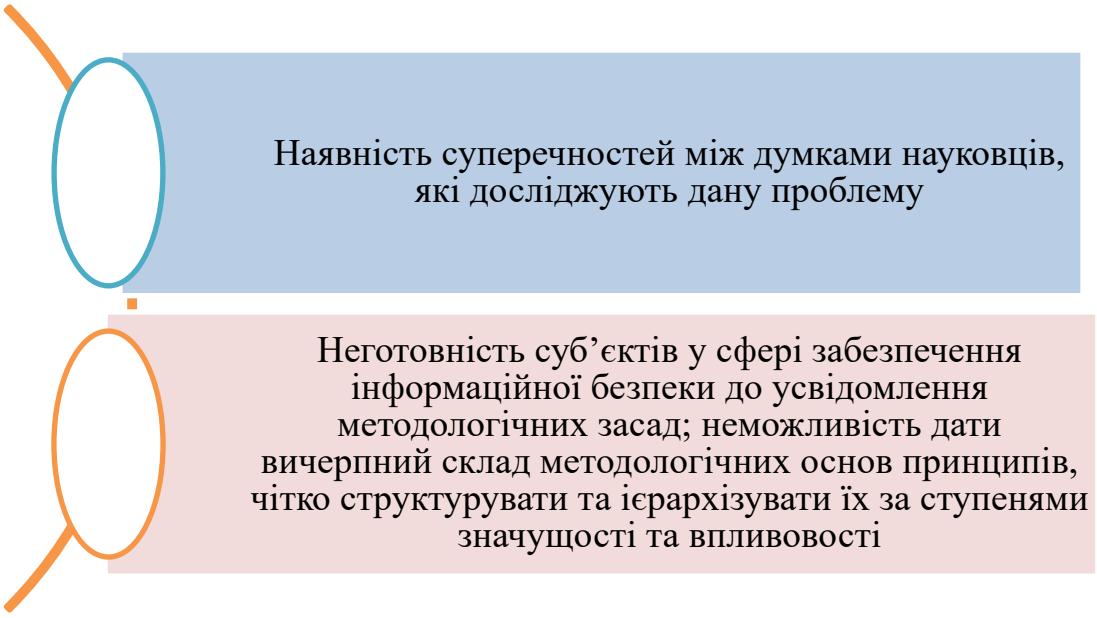

Рис.1.2. Основні причини проблеми визначення методологічних засад управління забезпеченням інформаційної безпеки

Примітка: побудоване автором на основі джерела [12, с. 76]

Як відомо, по суті, будь-який принцип управління як соціальне явище має конкретну мету і відповідне змістове навантаження. Спільні для всіх принципи управління «є їхня здатність визначити тенденції відтворення певних характеристик об'єкта незалежно від конкретних умов. Тому управляти інформаційною безпекою на підставі наведених принципів означає знаходити наявні й потенційні можливості забезпечувати на практиці формування визначених характеристик об'єкта у часі та просторі. Обгрунтування певної системи принципів управління забезпеченням інформаційної безпеки означає підвищення методологічного рівня організаційної адекватності інформаційної безпеки соціально-економічному станові держави. Грунтуючись на міцних методологічних засадах, інформаційна безпека держави починає функціонувати саме як системне утворення» [12, с. 77].

Залежно від природи принципи права поділяються на соціально-економічні, політичні, ідеологічні, релігійні, естетичні та спеціально-правові. Особливістю останніх є те, що вони, за існуючою думкою, відповідають на

питання, як право відображає його соціальну основу, яка структура права і яка природа правового регулювання суспільних відносин.

В. Колпаков, при розгляді принципів державного управління звертає увагу на те, що «принципи державного управління – це його позитивні закономірності, які пізнані наукою і практикою, а також охарактеризовані (зафіксовані, закріплені) у відповідних поняттях, що ознаками принципу управління є: належність до пізнаних позитивних закономірностей; зафіксованість, закріпленість у суспільній свідомості, що здійснюється у правовій формі, найчастіше у вигляді відповідних юридичних норм» [14, с. 312].

Таблиця 1.2. Принципи державного управління

Назва	**Складові**
«Соціально-політичні»	«демократизм, участь населення в управлінській діяльності держави; рівноправність осіб різних національностей; рівність усіх перед законом; законність; гласність і врахування громадської думки; об'єктивність»
«Організаційні принципи побудови апарату державного управління»	«галузевий, функціональний, територіальний»
«Організаційні принципи функціонування апарату державного управління2	«нормативність діяльності, єдиноначальність, колегіальність, поділ управлінської праці; відповідальність за прийняті рішення; оперативна самостійність»

Примітка: побудоване автором на основі джерела [14, с. 313].

Б. Кормич, «пропонує для визначення принципів забезпечення інформаційної безпеки два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу, а саме: це комплекс питань, пов'язаних з інформаційною безпекою людини і суспільства, яка, в першу чергу, вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення; це комплекс питань, пов'язаних з інформаційною безпекою держави, які, навпаки, пов'язані із застосуванням обмежень, заборон,

жорсткою регламентацією певних типів відносин в інформаційній сфері і невід'ємним елементом яких є сила державного примусу» [16, с. 201].

А. Стрельцов, «принципи діяльності із забезпечення інформаційної безпеки розділяє на загальні та особливі. До загальних принципів він відносить гуманізм, соціальну справедливість, об'єктивність, конкретність, ефективність, опора на підтримку і довіру народу, поєднання гласності і професійної таємниці, законність і конституційність. До особливих принципів із забезпечення інформаційної безпеки він відносить, насамперед, принцип глобальності» [24, с. 154].

Колектив авторів «Методи інформаційної безпеки» Ю. Уфімцев, В. Буянов, Е. Єрофеєв та ін., найважливішими принципами визначають: «законність заходів із виявлення і попередження правопорушень в інформаційній сфері; безперервність реалізації і вдосконалення засобів і методів контролю і захисту інформаційних систем; економічна доцільність, тобто співставлення можливих збитків і витрат на забезпечення безпеки інформації; комплексність використання всього арсеналу засобів захисту на всіх етапах інформаційного процесу» [27, с. 401].

А. Логунов звертає увагу на те, що «загальновизнаним у світі фундаментом міжнародного права є статут ООН, що цілі, принципи та інші настанови ООН є основою чинного міжнародного права. Статут ООН займає вищу позицію в ієрархії міжнародно-правових норм, які регулюють різні аспекти міжнародного життя, в тому числі й міжнародну безпеку. Статут ООН закріпив мету сприяння економічному і соціальному прогресу всіх народів» [17, с. 109].

Основну мету інформаційної безпеки слід визначати на основі широкого розуміння цього поняття як важливої складової національної безпеки та системоутворюючого фактора в усіх сферах життя, суспільства, держави, політичної, економічної, соціально-культурної, наукової. та технологічна, оборонна, екологічна, інформаційна та інші складові. національна безпека.

Таким чином, «головна мета державної політики інформаційної безпеки має полягати у захисті: конституційних прав і свобод людини і громадянина, забезпеченні єдності їх прав і обов'язків; духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності, інформаційної безпеки в політичній, економічній, соціокультурній, науково-технологічній, оборонній і державної безпеки, екологічній, власне інформаційній тощо складових національної безпеки» [17, с. 110].

Принципи формування та забезпечення функціонування системи інформаційної безпеки «мають бути спрямованими на реалізацію головної мети державної політики та визначатися законом як важливіші складові правових механізмів регулювання відносин у цій системо-утворюючій складовій забезпечення національної безпеки» [17, с. 111].

Національна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих у встановленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, військовій, екологічній, науково-технічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України зумовлений необхідністю своєчасного вжиття заходів, адекватних характеру та масштабу загроз національним інтересам [3].

Таким чином, ми пропонуємо визначити такі принципи інформаційної безпеки:

- «пріоритет прав, свобод і законних інтересів людини і громадянина»;
- «верховенство права, рівність усіх суб'єктів правовідносин перед законом»;
- «відповідальність держави перед людиною за свою діяльність»;
- «комплексний підхід до вирішення завдань забезпечення інформаційної безпеки»;

- «єдність і взаємозв’язок напрямів забезпечення інформаційної безпеки»;
- «розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки»;
- «участь у міжнародних і регіональних системах інформаційної безпеки»;
- «оперативність, своєчасність, превентивність і адекватність заходів щодо попередження і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз» [15, с. 14].

Отже, охарактеризувавши принципи забезпечення інформаційної безпеки України, варто зазначити, що ми запропонували основні загальні принципи інформаційної безпеки, тобто її формування та функціонування. Ми не претендуємо на вичерпність запропонованих принципів і вважаємо, що розвиток цивілізації, науково-технічного прогресу, глобалізація та загострення проблем, пов’язаних із безпекою життєдіяльності народів, неминуче вимагатимуть пошуку нових підходів до їх вирішення.Ми також вважаємо, що запропоновані принципи допоможуть уникнути фрагментації та формування національної системи інформаційної безпеки. Ці принципи забезпечення інформаційної безпеки є основою формування та функціонування системи інформаційної безпеки як системоутворюючого чинника всіх складових національної безпеки, норм і правил поведінки громадян, державних і громадських інститутів України у цій сфері.

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

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

Аналізуючи нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині, варто зауважити, що серед багатьох міжнародно-правових актів зрозуміло, що інформаційна та мережева безпека розуміється як здатність мережі або системи протистояти певному рівню надійності аварій або зловмисних дій, які можуть порушити доступність, цілісність та конфіденційність інформації, що зберігається або передається. , а також послуги, що надаються через мережу або інформаційну систему. Безпека визначається як доступність, ідентифікація, цілісність, конфіденційність інформації. Особлива увага приділяється правовій базі, яка впливає на перехоплення та розшифровку інформації [21, с. 131].

Одним із найдавніших законів вважається Закон «Про свободу друку» 1776 року прийнятий в Швеції, який «передбачає право доступу громадян до інформації про діяльність органів державної влади, і в даний час сфера його дії поширюється на всі види документів, включаючи електронні».

У ряді європейських країн, таких як Нідерланди, Іспанія, Португалія, Австрія, Угорщина, Естонія, Бельгія та Румунія, право громадян на доступ до офіційної інформації закріплено в конституції. У Франції, Греції та Італії ці права закріплені законом. Законодавство у цій сфері вдосконалюється у Великобританії, Німеччині, Естонії, Молдові, Польщі та ряді інших країн.

Так, у Швеції і Фінляндії «законодавчо встановлено обмеження прав на доступ до урядової інформації. Сьогодні важливо відзначити і іншу тенденцію в зарубіжних країнах, як втім і в Україні, – це розробка і реалізація концепцій електронного уряду, що ґрунтується на застосуванні

інформаційних технологій при створенні державних інформаційних ресурсів та доступу до інформації про діяльність державних органів влади, відкритих даних» [21, с. 132].

В Австрії, наприклад, право громадян на доступ до законодавчої бази також закріплено законодавчо, причому інформація є у розпорядженні державного сектора, а не комерційних структур (стягується плата за копіювання та розповсюдження).

Таким чином, аналіз зарубіжного досвіду правового регулювання доступу до інформації показує не лише загальні тенденції, а й різні підходи до правового регулювання інформаційної безпеки.

Значний набір законів і нормативних актів у сфері інформаційної безпеки в багатьох зарубіжних країнах стосується електронної комерції та використання електронних підписів:

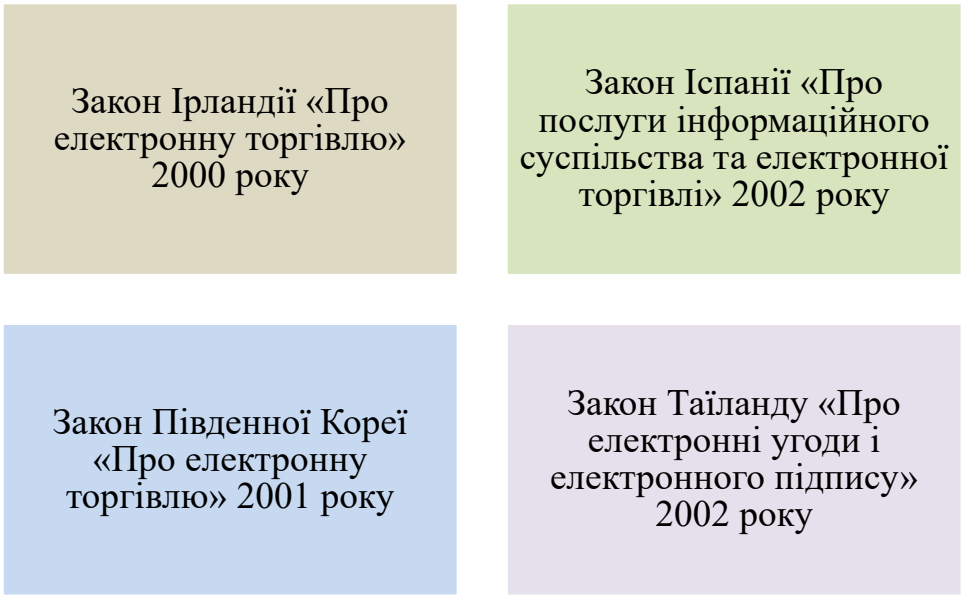

Рис.2.1. Набір законів і нормативних актів у сфері інформаційної безпеки в зарубіжних країнах

Примітка: побудоване автором на основі джерела [41].

Аналіз стану правового регулювання у цій сфері в розглянутих зарубіжних країнах показує, що нормативно-правові акти, що регулюють охорону інформації, інформаційних технологій та технологій, спрямовані на

створення та захист інформаційних мереж, встановлення єдиних умов використання ліній зв'язку та послуг зв'язку, є чинними.

Питання захисту персональних даних, що регулюються в багатьох державах, заслуговують на особливу увагу у сфері правового забезпечення інформаційної безпеки. Наприклад, в Іспанії ще в 1999 р був прийнятий Органічний закон «Про захист персональних даних», згідно з яким «загальнодоступними джерелами є: списки висунутих на посаду кандидатів, телефонні довідники (відповідно до законодавства) і списки осіб за професіями, що містять інформацію про імена, звання, професії, рід діяльності, а також офіційні видання, бюлетені і ЗМІ» [26, с. 178].

Однак слід зазначити, що «в Україні завершена майже семирічна процедура, пов'язана з ратифікацією одного з найактуальніших міжнародних правових актів у сфері захисту прав людини в процесі використання сучасних інформаційно-комунікаційних технологій – Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних 1981 р .

Таким чином, зроблено значний крок на шляху до повноформатної участі України в зусиллях держав – членів Ради Європи зі зміцнення безпеки людини в кіберпросторі та загальноєвропейському правовому просторі.

Однак процес модернізації зазначеної Конвенції, в якому Україна задіяна в якості повноправного учасника, все ще триває, чим і викликане динамічний розвиток, видання підзаконних актів та інших нормативно-правових актів»[26, с. 179].

Однією з найактуальніших зараз у світі є «проблема правового регулювання в мережі Інтернет. Глобальна інформаційно-телекомунікаційна мережа Інтернет поряд з об'єктивними благами, які вона дає людству, ввібрала в себе багато проблем суспільства, що проявилися у виникненні нових форм (видів) протиправної діяльності і виникнення нових загроз, несумісних із завданнями підтримки світової стабільності і безпеки. Завдання щодо забезпечення протидії тероризму і екстремізму відображені в державній політиці багатьох зарубіжних держав, і аналіз правового

регулювання в цій сфері дозволяє зробити висновок про тенденцію до посилення відповідальності за кібертероризм і поширення протиправної інформації» [15, с. 11].

У 2001 році Європейська комісія представила документ, під назвою «Мережева та інформаційна безпека підхід європейської політики», в якому висвітлювався нинішній підхід ЄС до інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який інтерпретується як здатність мережі або інформаційної системи протистояти випадковим подіям або зловмисним діям, які загрожують доступності, справжності, цілісності та конфіденційності даних, що зберігаються або передаються, та послуг, що надаються. . через ці мережі та системи» [44].

У документі визначено основні напрями європейської політики інформаційної безпеки «підвищення поінформованості користувачів щодо можливих загроз використання мереж зв'язку», «Створення європейської системи попередження та інформації про нові загрози», «Надання технологічної підтримки», «Підтримка ринкової стандартизації та сертифікації», «Юридична підтримка, пріоритетами якої є захист персональних даних, регулювання телекомунікаційних послуг та боротьба з кіберзлочинністю» «Посилення інформаційної безпеки на державному рівні шляхом впровадження ефективних та сумісних засобів забезпечення інформаційної безпеки та заохочення використання електронних підписів державами-членами при наданні загальнодоступних онлайн-послуг тощо»;

ЄС також приділяє особливу увагу кібербезпеці як невід'ємній частині інформаційної безпеки. З 1999 року ЄС реалізує програму «Найбезпечніший Інтернет», яка «вживає заходів не лише для боротьби зі шкідливим контентом, але й з небезпечною поведінкою в Інтернеті» [63].

У 2007 році Європейська комісія представила документ «На шляху до загальної політики кіберзлочинності», в якому кіберзлочинність визначається як кримінальний злочин, вчинений з використанням мереж та інформаційних систем електронного зв'язку або проти таких мереж та систем, і включає:

традиційні злочини (шахрайство та підробка документів)). у мережах електронних комунікацій та інформаційних системах), Публікація нелегального контенту у електронних ЗМІ, конкретні правопорушення в електронних мережах (атаки на інформаційні системи, злом та ін.)» [45].

У 2009 році Європейська комісія опублікувала повідомлення, озаглавлене «Захист Європи від великомасштабних кібератак та руйнувань підвищення готовності, безпеки та стійкості, в якому було визначено ключові виклики/проблеми, які необхідно негайно вирішити ЄС, та викладено заходи. необхідно для зміцнення безпеки та здатності критично важливої інформаційної інфраструктури Європи протистояти зовнішнім впливам» [44].

Зокрема, у Резолюції Генеральної Асамблеї ООН про право на недоторканність приватного життя в епоху цифрових технологій від 18 грудня 2013 року наголошується на глобальному та відкритому характері Інтернету та швидкий розвиток інформаційних та комунікаційних технологій як рушійної сили прискорення прогресу на шляху до розвитку в різних сферах. поля. форми. Документ підтверджує, що «ті самі права, які люди мають офлайн, мають бути захищені онлайн, включаючи право на недоторканність приватного життя» [52].

Зокрема, це типово для німецького законодавства: «Детальна розробка системи різних типів інформації з обмеженим доступом, чітке формулювання їх ухвал у федеральному законі». Таким чином, згідно із Законом про інспекцію безпеки секретна інформація - це факти, продукти та інформація, незалежно від форми їх подання, які мають зберігатися у секреті у суспільних інтересах та надаватися державним органом або від його імені певною мірою секретності потрібен відповідний рівень захисту» [53].

У жовтні 1997 року в Німеччині було прийнято Закон про захист телекомунікаційної інформації (TDPA). Відповідно до його загальних принципів збір, обробка та використання інформації дозволені лише у випадках, коли це дозволено законом або за згодою користувача. Інформація може збиратися, оброблятися або використовуватися окремо лише для різних

послуг, запрошених одним і тим самим користувачем, та згода користувача не є умовою для надання послуг» [68].

«Водночас у Німеччині з 2005 року діє Закон про свободу інформації, який регулює доступ до інформації. На уповноваженого за інформацією та захистом персональних даних покладено нагляд за виконанням положень цього нормативного акта. З 1990 року в країні діє закон про доступ людей та дослідників до архівів Штазі, колишньої служби безпеки Східної Німеччини» [65].

«Федеральна служба інформаційної безпеки, як і Закон Німеччини про посилення безпеки інформаційних систем, відіграє провідну роль у забезпеченні безпеки інформації в Німеччині у співпраці з приватним сектором, що ґрунтується на цьому агентстві. Усі вони є членами Федерального міністерства внутрішніх справ, яке, крім іншого, забезпечує внутрішню безпеку та захист конституційного ладу Німеччини, бореться з тероризмом, екстремізмом, шпигунством та саботажем. Відповідно до Закону «Про Федеральне управління безпеки інформаційних систем» VSI збирає та оцінює інформацію про загрози державній кібербезпеці, виявляє нові види кібератак» [40].

У співпраці з НАТО та ЄС також покладаються такі функції, як «оцінка ризиків впровадження інформаційних технологій; розробка критеріїв, методів та засобів перевірки для оцінки безпеки національних систем зв'язку, перевірка безпеки комп'ютерних систем та видача відповідних сертифікатів, видача дозволів на впровадження інформаційних систем у важливих державних установах, здійснення спеціальних заходів безпеки під час обміну інформацією у держструктурах, поліції та ін., консультування представників галузі з питань інформаційної безпеки. Крім того, Агентство просуває потребу в інформаційній безпеці» [67].

З метою оптимізації оперативної співпраці між усіма державними установами та покращення координації заходів щодо боротьби з кібератаками в Німеччині на базі Федерального управління безпеки

інформаційних систем, Національного центру кіберзахисту (NCAZ), який «безпосередньо взаємодіє з іншими суб'єктами кібербезпеки, включаючи приватний сектор, країни-партнери ЄС, НАТО та міжнародні організації» [67].

Федеральне управління захисту конституції також відповідає за інформаційну безпеку Німеччини (VFV) та Управління інформаційних операцій, «створене в 2009 році в бундесвері в результаті масованих атак на комп'ютерні мережі державних структур Німеччини в лютому 2009 року» [74].

Також наприкінці 2010 року в рамках реалізації концепції кіберзахисту у структурі командування Бундесверу було створено Групу операцій з інформацією та комп'ютерними мережами, яка працює з 5 квітня 2017 року під назвою Cyber Німецько-інформаційні космічні сили завершено. До завдань відповідного підрозділу входять, зокрема «розробка нових методів кібератак, проникнення в комп'ютерні мережі іноземних держав та організацій з метою отримання інформації, здійснення операцій деструктивного впливу на автоматизовані мережі та системи або блокування їх діяльності» [50].

Національна інформаційна політика Республіки Польща «орієнтована на побудову відкритого вільного суспільства, забезпечення прав людини, реалізацію концепції вільного транскордонного переміщення інформації, створення незалежних та плюралістичних засобів масової інформації». Його правова основа – «Закон про пошту та телекомунікації, Закон про радіомовлення та телебачення, Закон про державні відносини з Римо-католицькою церквою в Республіці Польща, прийнятий у 1990-х рр. (49% іноземного капіталу), ліцензування інформації про види діяльності. Права церкви на інформаційну діяльність встановлюються окремо» [58].

«Агентство внутрішньої безпеки відіграє ключову роль у забезпеченні кібербезпеки Польщі (ABW). У 2013 році ABW «розробила польську стратегію кібербезпеки та ініціювала створення Центру криптології при

Міністерстві національної оборони, який відповідає за захист інформації, кіберзахист та наступальні кібероперації» [38].

ABW також «створила урядову групу реагування на IT-інциденти (CERT)» [47], основне завдання якого полягає в «забезпеченні та розвитку потенціалу державного управління із захисту від кіберзагроз, зокрема від атак на інфраструктуру, що складається з комп'ютерних систем та комп'ютерних мереж, порушення чи знищення яких може серйозно загрожувати життю та здоров'ю». «Люди, національне багатство та навколишнє середовище або призводять до значних фінансових втрат та збоїв у функціонуванні органів державної влади» [12, с. 76].

«У зв'язку з ескалацією гібридних інформаційних загроз, таких як пропаганда, дезінформація або психологічне залякування з боку інших країн та недержавних суб'єктів (тероризм та інші організації), Управління національної безпеки Польщі (BBN) у 2015 році розпочало роботу над Польською доктриною інформаційної безпеки. Загрози інформаційної безпеки в доктрині включають ескалацію напруженості у міжнародних відносинах, дискредитацію міжнародної політики Польщі та формування негативного іміджу Польщі на міжнародній арені, у тому числі серед союзників по НАТО чи ЄС, формування іміджу Польщі як країни ксенофобів та антисемітів та провокацію польсько- польської меншини у Литві» [6].

Якщо говорити про захист інформації з обмеженим доступом, слід зазначити, що «після вступу до НАТО Польща, а також Чехія та Словаччина розробили нове законодавство щодо захисту секретної інформації, засноване на нових принципах. Так, у січні 1999 р. набув чинності Закон про захист конфіденційної інформації, прийняття якого стало умовою вступу Польщі до НАТО. Закон застосовується до секретної інформації та даних, що збираються державними органами, розкриття яких може завдати шкоди державі або громадським інтересам, або захищеним законом інтересам громадян чи організацій» [58].

На відміну від Польщі, «Угорщина адаптувала чинне законодавство

НАТО для захисту державної та службової таємниці. Зокрема, у 1995 р. Угорщина ухвалила закон про державну та службову таємницю, в який у 2001 р. були внесені поправки та виправлення, засновані на практиці Альянсу» [58].

Угорщина стала першою постсоціалістичною країною, яка ухвалила закон про захист особистих даних, Закон 1992 року про захист особистої інформації та доступ до інформації, що становить суспільний інтерес, внесений комісаром парламенту із захисту інформації та свободи інформації [59].

Відповідно до цього закону, будь-яка інформація, оброблена органами, які «виконують громадські обов'язки», становить суспільний інтерес, за винятком особистої інформації. Однак доступ та поширення інформації про діяльність політиків та державних службовців не можуть бути обмежені на підставі захисту особистої інформації. Закон також зобов'язує державні органи надавати громадськості точну та своєчасну інформацію та дає угорським громадянам право вимагати доступу до інформації, що становить суспільний інтерес. У цьому випадку особисті дані можуть збиратися та оброблятися лише з відома зацікавленої особи або відповідно до закону».

«Питання забезпечення інформаційної безпеки в Угорщині, у тому числі кібербезпеки, також регулюється Законом про електронну інформаційну безпеку державних та муніципальних органів від 2013 року та параграф 31 «Стратегії національної безпеки Угорщини», затвердженої у 2012 році» [54].

У Стратегії національної безпеки, зокрема, йдеться, що «Угорщина має бути готова до управління ризиками та загрозами, пов'язаними з інформаційною безпекою, обороною, боротьбою зі злочинністю та запобіганням кіберзлочинам, а також до забезпечення належного рівня безпеки. безпеку та інші завдання, пов'язані з кібербезпекою. Основне завдання – систематичне визначення пріоритетів у сфері потенційних загроз та ризиків у кіберпросторі, а також підвищення поінформованості про них.

Відповідні положення набули подальшого розвитку у Угорській національній стратегії кібербезпеки, затвердженої у 2013 році» [61].

У Хорватії з 2007 року діє «Закон про інформаційну безпеку», який визначає концепції інформаційної безпеки, заходи та стандарти інформаційної безпеки, а також інформаційну безпеку та компетентні органи для прийняття та реалізації рішень у галузі інформаційної безпеки та дотримання нормативних вимог. стандарти. Зокрема, інформаційна безпека визначається як стан конфіденційності, цілісності та доступності інформації, що досягається за рахунок реалізації політик та стандартів та організаційної підтримки зайнятості, планування, реалізації, оцінки та впровадження заходів та стандартів» [55].

Крім того, у 2015 році Хорватія ухвалила національну стратегію кібербезпеки. Стратегія кібербезпеки Хорватії заснована на наступних принципах «комплексний підхід до кібербезпеки, що охоплює кіберпростір, інфраструктуру та користувачів відповідно до хорватської юрисдикції (громадянство, реєстрація, домен, адреса)», «Інтегруючі заходи у різних галузях інформаційної безпеки», «Підвищення стійкості, надійності та керованості шляхом застосування універсальних критеріїв конфіденційності, цілісності та доступності для певних груп інформації та соціальних цінностей»; «Захист права і свободи людини у кіберпросторі, зокрема - недоторканності приватного життя та власності», «Постійне вдосконалення правової бази»; «Субсидіарність при розподілі влади»; «Пропорційність витрат за кібербезпеку і рівень ризику тощо» [69].

Отже, проаналізувавши правове регулювання інформаційної безпека в Німеччині, Польщі, Хорватії та Угорщині, слід зазначити, що європейські країни зараз вважають вирішення проблеми інформаційної безпеки особистості, суспільства, держави, їхнього захисту від внутрішніх та зовнішніх загроз, у тому числі гібридів, одним із найважливіших стратегічних пріоритетів національної безпеки. Проблеми інформаційної безпеки особистості, суспільства, держави, їх захисту від різних загроз, як

зовнішніх, так і внутрішніх, в даний час займають одне з перших місць у пріоритетах державної політики та стратегії національної безпеки Центральної Європи, на яку наголошується на відповідних стандартах ЄС. та НАТО.

2.2. Характеристики інформаційної безпеки в органах державної влади (досвід США)

Аналізуючи забезпечення безпеки інформації у державних органах (досвід США), слід звернути увагу, на те що «Національна безпека США зазвичай визначається документом, званим як стратегією національної безпеки США (РНБ), який розробляється окремою адміністрацією кожного нового президента та поєднує зовнішню політику, національну оборону, міжнародні економічні відносини та політику допомоги розвитку. Нова версія нової NSS була нарешті випущена у грудні 2017 року і виявилася однією з найдовших стратегій в історії США – як мінімум удвічі довше, ніж попередня версія, опублікована у 2015 році» [72].

Цілком логічно послатися, перш за все, на досвід інформаційної безпеки, накопичений найвпливовішим з політичного, економічного та військового погляду - США.

З погляду інформаційної безпеки США можна вважати піонером, оскільки - це не лише перша країна у світі, яка запровадила електронний уряд із використанням новітніх інформаційних технологій, а й створила спеціальну систему захисту національної інформації, суверенітет та безпека, інформаційні ресурси.

«Посилаючись безпосередньо на характеристики американської моделі управління інформаційною безпекою, слід зазначити, що у США є кілька інститутів інформаційної безпеки - це агентство національної безпеки (АНБ), Національне управління кібербезпеки Міністерства внутрішньої безпеки

США, Федеральне бюро. відділу розслідувань (ФБР) Центрального розвідувального управління (ЦРУ)» [72].

Слід зазначити, що «серед державних інститутів інформаційної безпеки ANS також розвиваються партнерські відносини з приватним сектором та дослідницькими установами у формі планування заходів щодо боротьби з загрозами, що виходять від недержавних комп'ютерних мереж (отже, держава бере участь у захисті критиків приватних телекомунікаційних мереж, , електрика та банківська справа), телекомунікації, електричні мережі, мережі банківських розрахунків та провайдери інтернет-послуг, понад 150 державних організацій і навіть більше приватних, що координуються ANS»[72].

Водночас найважливішим інститутом, який забезпечує дотримання державного регулювання інформаційної безпеки, є президент США.

Існуюча організаційна та правова база для захисту національного інформаційного простору виходить з інформаційної підтримки політики безпеки та функціонування систем захисту та управління на користь вищої влади [34].

Базові правові рамки інформаційної безпеки США сформувалися після Другої світової війни, коли «американська інформаційна система зіткнулася з руйнівним впливом радянської пропаганди. Законодавство США про структурну інформаційну безпеку складається з федеральних законів та законів штату. Незважаючи на значні відмінності між законами штатів, інформаційне право є одним із найбільш уніфікованих, оскільки в американському суспільстві існує розуміння, що інформаційна безпека штату є ключем до безпеки кожного громадянина» [34].

Правовий основою управління інформаційної безпекою США є Закони про захист особистої таємниці (1974 р.), Закон про секрети (1974 р.), Державне покриття право на фінансову таємницю (1978 р.). «Про доступ до інформації про діяльність ЦРУ» (1984), «Про безпеку комп'ютерних систем» (1987), «Про шахрайство та комп'ютерне зловживання» (1986). З ініціативи

президента США Рейгана було розроблено та прийнято Закон про свободу інформації, та інформаційна безпека стала пріоритетом для Держдепартаменту. Згодом, у 1987 році, було прийнято Закон MB HR-145 «Про комп'ютерну безпеку», правила якого лягли в основу майбутнього законодавства про кібербезпеку. Вперше у правовій системі США.

З 2001 року, коли тодішній президент Буш звернувся до співробітників ЦРУ, заявивши, що «інформаційна безпека є головним пріоритетом національної безпеки США, країна починає здійснювати програми федерального уряду із захисту національної інформації». середовище у комп'ютерних мережах» [34].

Мета таких програм – «створити всебічно сприятливі умови для отримання та опрацювання спецслужбами інформації про загрози інформаційному потенціалу органів державного управління в інших державах та окремих особах. Крім прихованої інформаційної діяльності, значну увагу приділяють систематичному аналізу відкритих джерел та вилучення інформації з конфіденційних баз даних з використанням комп'ютерного обладнання. Він почав формувати правову базу для боротьби із кіберзлочинністю» [34].

Так, у 2003 році було реалізовано «Національну стратегію безпечного кіберпростору». Пізніше - Огляд політики кібербезпеки (2009 р.), Міжнародна стратегія кібербезпеки (2011 р.), Стратегія кібербезпеки критичної інфраструктури президента США (2013 р.), Проект стратегії покращення кібербезпеки критично важливої інфраструктури» (2014 р.), Закон про обмін інформацією (2015), «Стратегія національної безпеки» (2015), «Стратегія кібербезпеки Міністерства оборони» (2015). Положення цих документів охоплюють значний комплекс аспектів забезпечення безпеки мереж та електронних інформаційних ресурсів.

Під час президентства Барака Обами цифрова інфраструктура США була оголошена «стратегічною національною цінністю», а її захист – національним пріоритетом» [3].

В основу цієї тези «американський лідер поклав розвиток наукової доктрини. Це добре відома думка американського дослідника аспектів інформаційної безпеки Маршала МакКлюена про те, що у наш час економічні зв'язки та відносини все частіше набувають форми обміну знаннями, а не обміну товарами» [29, с. 220].

Найважливішим аспектом політики адміністрації Обами в галузі інформаційної безпеки була «тісніша співпраця держави та бізнесу, яка насамперед спрямована на захист публічних інформаційних ресурсів, а також усього американського інформаційного простору». «Це потребує втручання США у інформаційну сферу, у тому числі в інформаційний сектор економіки».

В результаті боротьба за людські ресурси, капітал та ринки стає другорядною «зараз головне - доступ до інформаційних ресурсів, знань, що призводить до того, що війни вже ведуться більше в інформаційному просторі і за допомогою інформації. зброю. Президент США склав список пріоритетних питань безпеки у стані інформаційної сфери: необхідність постійного вдосконалення та доопрацювання стратегії розвитку інформаційних та комунікаційних мереж, розвиток систем попередження та реагування на кібератаки, посилення громадської безпеки. приватне партнерство. у сфері інформаційної безпеки залучає інвестиції в інноваційні технології, роз'яснюючи широким верствам населення переваги необхідності боротьби з кіберзагрозами» [29, с. 220].

2010 року президент США підписав Комплексну національну ініціативу з кібербезпеки, яка органічно доповнила Військову доктрину США. Початок створення універсальної федеральної мережі захищених каналів зв'язку, яка «об'єднає всі центри швидкого реагування на кіберзагрози та атаки хакерів». «У центральному уряді США також створено спеціальні підрозділи кіберрозвідки для виявлення атак на мережі урядової розвідки та запобігання терористичним атакам. Також було розроблено систему управління ризиками для прогнозування ймовірних наслідків

несанкціонованого втручання в інформаційні мережі державних органів» [25, стор 152].

Впроваджено програму спеціальної програмної платформи «Ейнштейн», яка призначена для виявлення перешкод у державних інформаційних мережах. З квітня 2012 року хакерська атака в США класифікується як озброєна агресія і передбачає повний арсенал заходів у відповідь. Вражає, що сьогодні у США 25% коштів, отриманих на дослідження та розробки, йде на розробку систем захисту інформації. Це дуже важливі кошти, і не кожна держава у сучасному світі може їх собі дозволити».

Більше того, ці документи можна вважати офіційною національною політикою США в галузі інформаційної безпеки, в основі якої лежить система державної влади у цій сфері та структура державних органів, які забезпечують інформаційну безпеку у державі.

Відповідно до стратегії інформаційної безпеки, основними пріоритетами держави у цій сфері є (рис. 2.2.):

Рис.2.2. Головні державні пріоритети стратегії інформаційної безпеки у США

Примітка: побудований автором на підставі джерела [71].

Було визначено пріоритети національної інформаційної політики США:

«підтримка досліджень та розробок у галузі інформації та комунікації», «Вплив на їх напрямок та заохочення поширення технічних знань та можливостей в економіці», «Сприяння обміну технологіями між лабораторіями та компаніями, впровадження інновацій на ринки», «Створення та покращення інформаційної інфраструктури, контроль її діяльності, побудова глобальних систем зв'язку та дослідження впливу систем на міжнародні, національні та приватні пріоритети», «Підтримка балансу, досягнутого новими технологіями між чотирма основними інформаційними цінностями: конфіденційність інформації, інформація як суспільне благо, інформація як товар» [34].

Нова національна кіберстратегія (NCS) була розроблена відповідно до Указу президента № 3813800 від 11 травня 2017 р. «Посилення кібербезпеки федеральних мереж та критично важливої інфраструктури», який було опубліковано у вересні 2018 р. [71] Цей документ містить аналогічні цілі. з тими, що викладені в аналогічних попередніх документах: політика адміністрації Обами щодо кіберпростору 2009 р. [70] та «Стратегія національної безпеки Буша» 2002 р. про кібербезпеку» [73].

«Однак, незважаючи на подібність до попередніх адміністрацій, NCS Трампа знову викликав «критичну критику з боку його опонентів», тому що замість того, щоб продовжувати консолідувати технології безпеки та мінімізувати вплив інформаційних загроз, адміністрація президента має намір посилити наступальні та примусові кібероперації. інші. Країни побоюються кримінального переслідування за свої дії у відповідь на подібні кібератаки з боку США. Критики також зазначили, що дана стратегія жодним чином не вказує на можливість захисту виборів від інформаційних загроз, що надзвичайно актуально у світлі подій 2016 року» [75] .

У політиці США кульмінацією порушення інформаційної безпеки в США та символічною відправною точкою у його сучасному описі є «втручання Росії у президентські вибори у США 2016 року. Це безпрецедентно, тому що така великомасштабна російська кампанія, яка була

успішно проведена, зажадала місце вперше в контексті історії інформаційної безпеки США. Це був значний удар не лише по розвідці та національній безпеці країни, а й по її американській ідеології та іміджу».

«Представники влади та спецслужб США неодноразово заявляли, що авторитарна Росія намагалася вплинути та вплинути на президентські вибори у США. Так, у червні 2016 р. американські ЗМІ отримали інформацію про несанкціоноване втручання в інформаційну систему Національного комітету Демократичної партії США, зокрема російського «Агентства інтернет-досліджень» (IPA), яке фінансує Євген Пригожин» [9, с.88].

«Для багатьох американців таке втручання в інформаційний простір їхньої країни стало несподіванкою, хоча для російського уряду це була довгоочікувана спланована атака, яку він вважав виправданою роками подібних викликів із боку США, Клінтон і Д. Трамп, як відомо, були останніми кандидатами на виборах, і демократи припускають, що якби не неодноразове «порушення» кампанії Клінтона за допомогою електронних листів, вкрадених російськими хакерами та розміщених на WikiLeaks та антивірусних програмах. Повідомлення Клінтона, об'єктивно спрямовані на підтримку Трампа і які транслюються в соціальних мережах російськими IT-фахівцями, ситуація може змінитися. Проте президент Трамп та його адміністрація категорично не згодні з цією точкою зору» [64].

У 2017 році розпочалося розслідування втручання Росії у вибори під керівництвом спецпрокурора Роберта Мюллера. Розслідування ґрунтувалося на твердженнях про змову між російськими агентами та командою Трампа під час президентської кампанії та у перехідний період. У розслідуванні взяли участь такі структури, як ФБР, Сенатський комітет з розвідки, Постійний окремий комітет з розвідки, Судовий підкомітет Сенату з злочинності та тероризму, Комісія палати представників з нагляду та реформи та Судовий комітет Сенату. Розслідування показало, що втручання Росії у вибори здійснювалося за трьома напрямками: крадіжка та розголошення документів основних опонентів Трампа; масове шахрайство у

Facebook та Twitter з використанням антипропагандистських акаунтів Клінтон;

Слід зазначити, що остання пропозиція не була підтверджена, згідно з звітом Мюллера, який провів майже два роки біля керма групи експертів, які розслідували спроби Москви саботувати президентські вибори в США, і опублікував свій звіт про всяк випадок. «Він сказав. він не виявив змови, незважаючи на численні пропозиції росіян, які допомагали кампанії Трампа».

Загалом, до основних проблем, з якими стикаються Сполучені Штати в галузі інформаційної безпеки, належать «збільшення кількості установок шкідливого програмного забезпечення (вірусів) на мобільних пристроях, поширення вірусів шляхом розповсюдження неліцензійного програмного забезпечення в магазинах, крадіжка облікових записів та персоналу. Дата. Таким чином, встановлення вірусних програм на мобільні пристрої за 2018 рік збільшилося на 45%. Дослідження Symantec показало, що сторонні магазини програмного забезпечення виявили 99,9% шкідливих програм, які могли отримати доступ до особистих даних. Тільки в 2018 році в США було вкрадено близько 12 мільярдів облікових записів, які містять особисту інформацію, включаючи адресу, номер телефону, номер страховки або дані кредитної картки. Більше того, у тому ж 2018 році.

Таким чином, на основі наведеного вище матеріалу ми бачимо чітко окреслені виклики, з якими постійно стикаються Сполучені Штати як усередині країни, так і за її межами. Останні у комплексі мають суттєве дестабілізуюче значення для критично важливої інформаційної інфраструктури і тому становлять серйозну загрозу національній безпеці держави, особи та суспільства загалом. Це є відображенням неефективної політики уряду в контексті захисту даних та інформаційної безпеки після вторгнення, а також міжпартійних суперечок, що продовжуються, у тому числі в Конгресі та в засобах масової інформації, які перешкоджають певному конструктивному прогресу. Основним завданням уряду в таких умовах має бути розробка та розвиток єдиного бачення державної політики в

галузі інформаційної безпеки з формуванням сильної системи захисту та постійним удосконаленням останньої для протидії зовнішнім та внутрішнім загрозам. консенсус між основними політичними силами Америки. Крім того, зосередження уваги урядових, корпоративних та громадських діячів на подоланні загальної проблеми позитивно вплине на загальний стан справ у Сполучених Штатах. Такі заходи запобіжать інформаційним атакам та зовнішнім когнітивним впливам на громадськість у майбутньому за умови згоди основних політичних сил США. Крім того, концентрація державних суб'єктів, Подолання загальної проблеми позитивно позначиться на загальному стані справ у США. Такі заходи запобіжать інформаційним атакам та зовнішнім когнітивним впливам на громадськість у майбутньому за умови згоди основних політичних сил США. Крім того, зосередження уваги урядових, корпоративних та громадських діячів на подоланні загальної проблеми позитивно вплине на загальний стан справ у Сполучених Штатах.

РОЗДІЛ 3.
УДОСКОНАЛЕННЯ УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Адаптація досвіду країн ЄС із забезпечення інформаційної безпеки

Аналізуючи досвід країн ЄС із системи забезпечення інформаційної безпеки, варто зауважити, що пошук певного балансу між повним державним контролем і ринковими законами, тобто поєднанням влади та ринкових сил, є головною ознакою інформаційної політики не лише в Північній Європі, а й в інших країнах Європейського Союзу. У той же час ЄС продовжує приділяти пильну увагу сьогодні приватизації та лібералізації ринку інформаційно-комунікаційних технологій.

Система інформаційної безпеки Франції є складовою національної безпеки, відповідно її основні принципи закріплені в Білій книзі з оборони та національної безпеки.

У 1972 році була опублікована перша Біла книга про національну оборону, в якій були викладені принципи оборонної політики Франції та основи стратегії ядерного стримування. Друга Біла книга, опублікована в 1994 році, зосереджувала увагу на припинення холодної війни та перенаправлення збройних сил на військові операції за межами національної території, що призвело до професіоналізації збройних сил.

Процес глобалізації та боротьби з тероризмом привели до розробки нової концепції стратегії національної безпеки, яка безперешкодно поєднує політику оборони, політику внутрішньої безпеки, зовнішню та економічну політику. Ця концепція була закріплена в третій Білій книзі з оборони та національної безпеки в 2008 році.

Цей новий підхід до формування стратегії національної безпеки Франції, який характеризується розширенням стратегічного мислення окрім оборони, був обумовлений глобалізацією, яка глибоко змінила основи міжнародної системи, ставши більш нестабільними та непередбачуваними, ніж у холодні часи. Війна та створювати нові загрози. різного характеру. З 2009 року це поняття включено до Кодексу оборони Франції.

Ще одна особливість білої книги з національної оборони та безпеки 2008 року полягає у тому, що вона визначає загрози для використання інформаційних систем та засобів масової інформації. Таким чином, характеризуючи загрозу масштабних атак на інформаційні системи, зазначається, що останні проникають через основні системотворчі ланки економічного та соціального життя.

Таким чином, «залежність від комунальних інформаційних систем, транспортної інфраструктури, продовольчої безпеки та навіть управління обороною робить сучасне суспільство та його безпеку вразливими для випадкових пошкоджень та цільових атак з боку комп'ютерних мереж. Загроза шпигунства та стратегічного впливу виправдовується широким використанням (м'якої сили) у міждержавних відносинах, маніпулюванням свідомістю через ЗМІ та Інтернет, досягненням наукового, економічного, оборонного потенціалу Франції та її території, небезпека культурної експансії» [10. с. 456.].

Четверта Біла книга була опублікована у 2013 році під головуванням Франсуа Олланда. П'ятий документ, під назвою «Стратегічний огляд оборони та національна безпека, був опублікований наприкінці 2017 року під головуванням Еммануеля Макрона» [10].

Defense Review приділяє значну увагу «інформаційним загрозам та заходам протидії. Таким чином, зазначається, що в кіберпросторі деякі атаки через їх масштаби і серйозність можуть бути класифіковані як озброєна

агресія. Труднощі з розподілом часток та поєднанням прямої дії з методами впливу та пропаганди дозволяють використовувати численні інструментальні сценарії для дестабілізації або підтримки більш простих операцій.

«Облік кіберзагроз та його еволюції тим паче складний, що «він може обмежуватися периметром захисту через заплутані питання та участі державних і приватних суб'єктів. У зв'язку з цим підкреслюється, що армії повинні повністю планувати та проводити операції у цифровому просторі до тактичного рівня в ланцюжку планування та проведення кінетичних операцій. Операції в цифровому просторі розширюють діапазон традиційних ефектів, доступних політичній владі, і використовують цифровість опонентів Франції, що зростає, як державних, так і недержавних. Ця здатність вимагає покращених та дуже гнучких людських ресурсів, а також постійної розробки конкретних технічних рішень» [62].

Крім того, для забезпечення безпеки інформації Defense Review допускає кібервійну, що означає оборонну або наступальну боротьбу у всьому цифровому середовищі проти урядових чи неурядових супротивників.

Стратегії національної безпеки, викладені у Білій книзі, становлять основу законів про військове планування. Сьогодні діє закон Франції «Про військове планування на 2019-2025 роки та інші оборонні положення» №2018-607 від 13.07.2018. Для Франції так званий «кіберджихадизм» залишається серйозною загрозою її інформаційному простору, який складається з використання інтернет-технологій та послуг, особливо соціальних мереж, для пропагування джихадистського насильства. Це робиться шляхом злому урядових веб-сайтів, корпоративних веб-сайтів або організацій, захисту інтересів та найму. Заходи протидії: блокування сайтів та облікових записів, створення сайтів контрпропаганди тощо.

Система інформаційної безпеки у Франції складається з таких спеціальних структур «Національного агентства з безпеки інформаційних систем (ANSSI)», «Аудіовізуальної служби (Audiovisual), Міжвідомчого

управління інформаційних систем та комунікацій (DISIC)», «Управління розвитку ЗМІ)» та інші деякі.

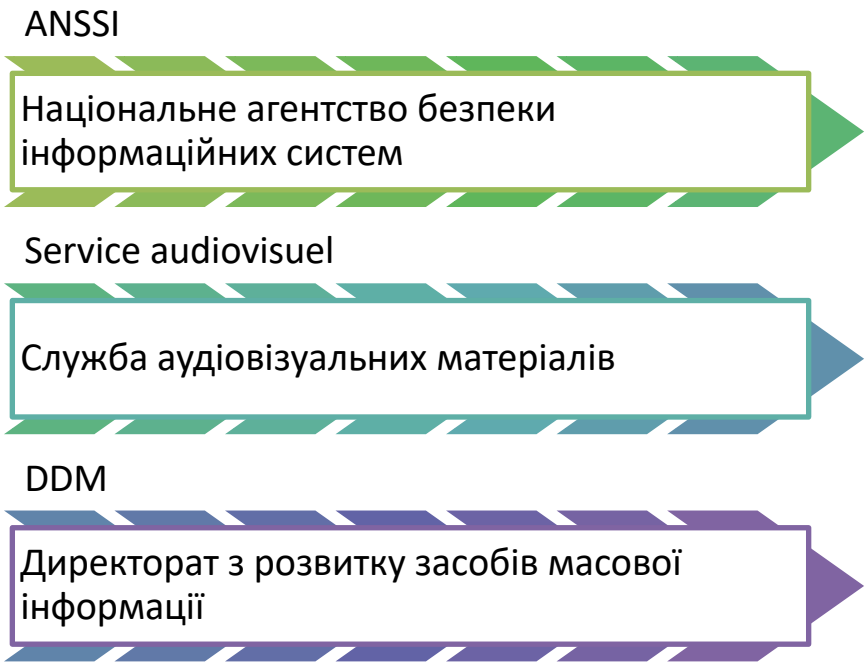

Рис.3.1. Система інформаційної безпеки у Франції

Примітка: побудована автором на підставі джерела [51]

Національне агентство безпеки інформаційних систем (ANSSI) – це «французька служба з національною компетенцією, створена указом у липні 2009 року під егідою Генерального секретаріату оборони та національної безпеки».

ANSSI відповідає за просування національних технологій, систем та досвіду для просування цифрової економіки. При цьому основні зусилля фахівців ANSSI спрямовані на реалізацію заходів, передбачених у стратегії національної безпеки та оборони. «Основними завданнями агенції є підвищення ефективності управління та координації органів державної влади, критичної інфраструктури, суспільства з погляду комп'ютеризації; забезпечення промислової безпеки, організація захисту національної розвідувальної та телекомунікаційної інфраструктури в умовах військової загрози, у тому числі кібервійни; підтримка технічних засобів, необхідних

для виконання завдань, поставлених перед Агентством у його нинішньому вигляді. У його повноваження входять» [51]:

- «формування державної політики у сфері захисту та безпеки інформаційних систем»;

- «розробка організаційних, правових та технічних заходів щодо захисту державних інформаційних систем та контроль за їх впровадженням»;

- «моніторинг, виявлення, повідомлення та реагування на кібератаки, спрямовані на державні інформаційні та телекомунікаційні системи»;

- виявлення та реагування на вірусні атаки, реалізація механізмів адаптивного захисту від них;

- «запобігання загрозам шляхом сприяння розробці надійного програмного та апаратного забезпечення»;

- «Консультації та підтримка об'єктів критичної інфраструктури»;

- «Систематичне інформування громадськості про загрози, зокрема через урядовий веб-портал з питань ІБ»;

- «розробка та придбання товарів, призначених для захисту найбільш уразливих ділянок міжвідомчої державної мережі»;

- «Здійснення контролю та комунікацій з питань національної оборони та безпеки»;

- «Сертифікація інтегрованих систем захисту інформації» [51].

Аудіовізуальна служба, яка діє під головуванням президента, також бере участь у реалізації інформаційної політики у Франції. Служба розробляє аудіовізуальні технічні платформи Президента Республіки, організує його виступи та забезпечує їх поширення по всій країні та за кордоном».

Крім того, Служба підтримує фотовідділ про діяльність президента та життя Єлисейського палацу, керує фотобанком та взаємодіє із засобами масової інформації та громадськістю. Важливою функцією цієї служби є аудіовізуальний моніторинг ЗМІ та формування адекватного архіву матеріалів. Загалом його діяльність спрямована на формування іміджу президента.

«У зв'язку з активною комп'ютеризацією органів державної влади у Генеральному секретаріаті уряду (SGG), що належить прем'єр-міністру, на початку 2011 року було створено Міжвідомче управління інформаційних систем та комунікацій (Постанова № 2022-193 від 21 лютого). 2011). (ДІСІК). Він відповідає за роботу інформаційних та телекомунікаційних систем для обміну інформацією між різними агенціями та з громадянами. Основними завданнями підрозділу є проектування державної інформаційної та телекомунікаційної інфраструктури з урахуванням потреб діяльності та оптимізації ресурсів, організація закупівель інформаційного обладнання, програмного забезпечення та послуг, розподіл електронних комп'ютерів між міністерствами, впровадження нових інформаційних систем» [10].

Метою створення DISIC є «відстеження тенденцій в інформаційних технологіях, оптимальне використання інформаційних ресурсів через загальні бази даних, запобігання ризикам інформаційної безпеки, пов'язаним з реалізацією великомасштабних проектів, покращення інформаційних систем обслуговування клієнтів» [10. с. 301.].

Основним законом у галузі інформаційної безпеки у Німеччині є Закон «Про посилення безпеки систем інформаційних технологій» (Information Security Law) від 25.07.2015. Закон відводить Федеральному управлінню інформаційних технологій (BSI) центральну роль захисту критично важливої інфраструктури у Німеччині.

Критичні інфраструктури – це установки, установки або їх частини, які «належать до секторів енергетики, інформаційних технологій та телекомунікацій, транспорту та дорожнього транспорту, охорони здоров'я, водопостачання, продовольства, фінансів та страхування. Такі об'єкти важливі для функціонування спільноти, оскільки їх закриття або погіршення стану спричинить значний брак матеріалів або створить загрозу громадській безпеці. 27 березня 2019 року Федеральне міністерство внутрішніх справ також опублікувало законопроект щодо безпеки інформаційних технологій, який містить цілісний підхід до безпеки у цій сфері.

Серед іншого, «передбачається запровадити простий у використанні ярлик комп'ютерної безпеки для комерційних продуктів, а також посилити компетенцію BSI та розширити список порушень кібербезпеки та пов'язаних із ними слідчих дій. Законопроект також збільшує кількість отримувачів звітів та зобов'язань. Загалом очікується, що закон створить певні економічні труднощі для підприємств та органів державної влади» [57].

«Інформаційна безпека у Німеччині забезпечується Федеральними збройними силами Німеччини (Бундесвер), зокрема, Відділом комп'ютерних мереж та інформаційних операцій Командування стратегічної розвідки. Командування стратегічної розвідки також керує системою розпізнавання супутників SAR-Lupe, яка була запущена у грудні 2008 року» [4].

Завдяки п'яти супутникам SAR-Lupe, які вважаються одними з найпередовіших систем у своєму роді, може передаватися зображення з роздільною здатністю менше одного метра, незалежно від денного світла та погоди. Таким чином, можна прояснити практично будь-яку точку Землі. Система збирає та оцінює інформацію про військово-політичну ситуацію в окремих країнах та альянсах потенційного чи поточного супротивника та його збройних сил.

Отже, проаналізувавши досвід Країни ЄС щодо системи інформаційної безпеки варто відмітити, що на сьогодні немає універсального підходу чи єдиної моделі управління інформаційної безпекою. У кожного регіону світу та країни є свої внутрішні особливості, які надалі визначають специфіку цього процесу. Системи інформаційної безпеки у Франції та Німеччині засновані на усвідомленні ризиків та загроз, пов'язаних із швидким розвитком інформаційних та комунікаційних технологій. Наприклад, одним з основних гравців у системі інформаційної безпеки у Франції є Національне агентство безпеки інформаційних систем (ANSSI), а в Німеччині – Управління інформаційних та комп'ютерних мереж Бундесверу.

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

Аналізуючи напрямки вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації, варто зауважити, що Інформаційна безпека України, на жаль, стикається з значними загрозами, викликами, які створюють загрозу функціонуванню держави, її політичному та економічному розвитку, інтеграції в європейські та євроатлантичні структури.

Загрози інформаційній безпеці України в інформаційній сфері – це «сукупність умов і факторів, які загрожують життєво важливим інтересам держави, суспільства та особи через можливість негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси. та інформаційна інфраструктура» [20, с. 90].

Як зазначено в Законі України «Про основи національної безпеки», однією з основних загроз інформаційній безпеці є спроби маніпулювати суспільною свідомістю, зокрема, шляхом поширення неточної, неповної чи упередженої інформації» [3].

Доктрина інформаційної безпеки України визначає такі загрози інформаційній безпеці країни «поширення у глобальному інформаційному просторі спотвореної, небезпечної та необ'єктивної інформації, яка завдає шкоди національним інтересам України», «Зовнішня деструктивна інформація впливає на суспільну свідомість через ЗМІ, а також через Інтернет»; «Деструктивний інформаційний вплив, спрямований на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України»; «Прояви сепаратизму в ЗМІ, а також в Інтернеті на етнічному, мовному, релігійному та іншому грунті» [32].

За словами Р.Р. Марутяна, «найсерйознішою загрозою національній безпеці України в інформаційній сфері є реалізація іноземними державами негативного інформаційного та психологічного впливу на суспільну

свідомість громадян України та світової спільноти за допомогою інформаційних кампаній та спеціальних розвідувальних операцій. Це пов'язано з систематичним поширенням необ'єктивної, неповної або необ'єктивної інформації про Україну та політичні процеси, що відбуваються на її території. Все це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичну та економічну основу. Метою цих інформаційних операцій є забезпечення національних інтересів інших держав» [19, з 89].

Загрози інформаційної безпеки України у сфері інформації також мають включати «прояви обмежень свободи слова та доступу до інформації для громадян», «Спотворення, спотворення, блокування, неявно упереджене та необ'єктивне висвітлення інформації», «Несанкціоноване поширення, відкрита дезінформація», «Поширення інформації іншими державами та деструктивне інформаційне вторгнення до національного інформаційного простору, коли країни з сильнішим інформаційним потенціалом мають можливість через ЗМІ розширювати свій вплив на населення та громадськість менш могутньої держави», «Виникнення та функціонування у національному інформаційному просторі стану неконтрольованих та інформаційних потоків тощо» [13].

Проти України широко використовуються сучасні технології негативного інформаційно-психологічного впливу, які стають загрозою для українського національного інформаційного простору та державного суверенітету. Забезпечення інформаційної безпеки України перед дестабілізуючим негативним інформаційним та психологічним впливом та агресивною експансіоністською інформаційною політикою Російської Федерації вимагає активізації зусиль на всіх рівнях влади та громадянського суспільства.

«Для протидії широко поширеним негативним інформаційним та психологічним впливам, операціям та війнам необхідно визначити пріоритетні напрямки державної інформаційної політики та важливі кроки з

боку української влади» [8. с. 106.]:

1) «Інтеграція України в європейський глобальний та регіональний інформаційний простір»;

2) «інтеграція в міжнародні інформаційно-розвідувальні та телекомунікаційні системи та організації»;

3) «створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства»;

4) «модернізація всієї державної системи захисту інформації, формування та реалізація ефективної інформаційної політики»;

5) «вдосконалення законодавства у сфері інформаційної безпеки, приведення національного законодавства у відповідність до міжнародних стандартів та ефективне регулювання інформаційних процесів»;

6) «розвиток національної інформаційної інфраструктури»;

7) «підвищення конкурентоспроможності внутрішніх інформаційних товарів та послуг тощо. д.» [8. с. 107.].

З метою запобігання розповсюдженню інформації державна діяльність в інформаційному просторі має здійснюватися за такими напрямками:

1) «реалізація превентивних стратегій та тактик (превентивних заходів)»;

2) «реалізація стратегії реагування (швидке реагування на атаки розвідки супротивника та активний наступ)»;

3) «захист національного інформаційного простору. Основна мета – забезпечити домінування та перевагу ЗМІ в інформаційному просторі».

Слід зазначити, що для захисту національного інформаційного простору, для створення ефективної системи захисту інформації українська влада вживає певних заходів. Зокрема, 14 січня 2015 року Кабінет Міністрів України ухвалив Постанову про створення Міністерства інформаційної політики України, пріоритетними завданнями якої є протидія інформаційної агресії з боку Російської Федерації; розробка ефективної державної стратегії інформаційної політики та Концепції інформаційної безпеки України;

злагодженість та узгодженість функціонування та діяльності органів державної влади та інформаційної сфери» [8. с. 109.].

З метою протидії негативним наслідкам інформаційної пропаганди та інформаційних воєн, нейтралізації та запобігання реальним та потенційним загрозам в інформаційному просторі України Рада національної безпеки та оборони України ухвалила рішення «Про заходи щодо вдосконалення навчання та реалізації державна політика інформаційної безпеки України».

У документі йдеться, що Рада національної безпеки та оборони, враховуючи необхідність удосконалення нормативно-правової бази та запобігання та нейтралізації потенційних та реальних загроз національній безпеці в інформаційній сфері, ухвалила іноземні держави, які передбачають, зокрема, визначення механізму протидії негативному інформаційному та психологічному впливу, зокрема заборона на ретрансляцію телеканалів, посилення контролю за дотриманням законодавства про інформаційну безпеку, психологічну та кібербезпеку, вжити заходів щодо того, щоб об'єктивна інформація про соціально-політичну ситуацію в Україні поширювалася по всьому світу» [2].

«Необхідність створення національної системи інформаційної безпеки очевидна, коли нею займатимуться відповідні підрозділи СБУ, кіберзахисту - відповідні підрозділи Державної служби спеціального зв'язку та захисту інформації та боротьби з кіберзлочинністю - відповідні підрозділи. Міністерства внутрішніх справ. Ефективну координацію та взаємодію забезпечуватиме відповідний підрозділ Ради національної безпеки та оборони» [30].

Національна система інформаційної безпеки створюється та розвивається відповідно до Конституції України та інших правових норм, що регулюють суспільні відносини у сфері національної безпеки, зокрема: Закон України «Про основи національної безпеки України», Концепція безпеки. та Національний координаційний центр розвитку оборонного сектору з кібербезпеки, Стратегії національної безпеки України, Стратегії кібербезпеки

України, Військової доктрини України, Доктрини інформаційної безпеки України та ін.

Кібервійна породжує нові кіберзагрози. Кіберзагрози – це «існуючі та потенційно потенційні явища та фактори, які ставлять під загрозу життєво важливі інтереси людини та громадянина, суспільства та держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційних та телекомунікаційних систем. [13, с.88].

Створення національної системи інформаційної безпеки забезпечується Стратегією кібербезпеки для безпечної експлуатації кіберпростору, його використання на користь особистості, суспільства та держави.

Організаційне забезпечення системи захисту інформації також можна розглядати як умисну діяльність суб'єкта захисту інформації, пов'язану з:

- «створення та оптимізація (розвиток) організаційних структур, що найбільш підходять для забезпечення кібербезпеки»;

- «оптимізація (коригування) процесу управління у сфері безпеки у кіберпросторі, забезпечення найкращих умов прийняття та реалізації відповідних управлінських рішень».

Національна система інформаційної безпеки має насамперед «забезпечувати взаємодію в галузі інформаційної безпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, підприємств, установ та організацій, незалежно від форми власності, що здійснюють діяльність у галузі електронних комунікацій, інформаційної безпеки та/або є власниками (адміністраторами) критичної інформаційної інфраструктури. Основою національної системи захисту інформації стануть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України [36].

Аналізуючи системи захисту інформації провідних країн світу, ми приходимо до висновку, що на сьогоднішній день не існує єдиної моделі побудови національної системи захисту інформації.

Стратегія кібербезпеки Канади «визначає кібертероризм і кіберворожі дії в інших країнах (кібершпигунство та кібервійни) як основні загрози кібербезпеці країни та ключовий орган, відповідальний за координацію та моніторинг реалізації цієї стратегії. І координацію кібербезпеки і протидія кібербезпеки» [7].

Австрійська стратегія кібербезпеки Центр кіберзлочинності Федерального міністерства внутрішніх справ Австрії був призначений національним координатором та центральним органом у галузі інформаційної безпеки. Крім того, на нього покладено основні функції правоохоронних органів у галузі інформаційної безпеки та боротьби з кіберзлочинністю.

«Агентство внутрішньої безпеки відіграє ключову роль у забезпеченні інформаційної безпеки Польщі (AVB) – «польський орган контррозвідки. Так, у 2013 році AVB розробила Польську стратегію інформаційної безпеки та ініціювала створення Центру криптології при Міністерстві національної оборони Польщі, завданням якого є захист інформації, кіберзахист та наступальні кібероперації (активний кіберзахист)» [36].

«Аналіз нормативно-правових та організаційних засад системи інформаційної безпеки у провідних країнах світу свідчить про домінуючу роль спецслужб у забезпеченні кібербезпеки держави у зв'язку з характером сучасних кіберзагроз. органи контррозвідки держави» [36].

«У світлі міжнародного досвіду та для того, щоб ефективно вирішувати питання державної кібербезпеки, агентство, яке координує діяльність усіх суб'єктів у галузі кібербезпеки (Національна система інформаційної безпеки), рекомендується призначити Службу безпеки України, яка є спеціально уповноваженим органом у галузі контррозвідки, а також протидії внутрішнім та зовнішнім загрозам, у тому числі в інформаційній сфері (кібернетика).

Також з урахуванням світової практики пропонувалося створити Національний центр кібербезпеки, який мав бути підпорядкований Службі безпеки України»12, с. 77].

Особливу увагу приділено «Національній системі інформаційної безпеки України» від Української служби реагування на надзвичайні ситуації – спеціалізованого підрозділу Державного центру захисту інформації та телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України, створеного у 2007 році. UA полягає у забезпеченні захисту державних інформаційних ресурсів та інформаційно-телекомунікаційних систем від несанкціонованого доступу, неправомірного використання та порушення їх конфіденційності, цілісності та доступності. Діяльність CERT-AU передбачена Законом України «Про державну службу спеціального зв'язку та захисту інформації», Законом України «Про зв'язок» та Положенням.

Україна має «створити ключові механізми державного управління інформаційною безпекою перед кіберзагрозою у вигляді спеціалізованих центрів, інститутів та експериментів з операціями інформаційної війни, фінансувати спеціалізовані дослідження в галузі розвідувальних операцій та створювати структури для досліджень та розробок.

На порядку денному – завдання «поступового становлення індустрії програмного забезпечення», «прискорити роботи зі створення Української національної мережі суперкомп'ютерних комплексів, поєднаних із високошвидкісними оптоволоконними каналами передачі даних», «формувати чітку інформаційну політику щодо просування місцевих IT-компаній за кордоном, об'єднати інтереси освіти, науки та IT-бізнесу», «визначення базових вузів, на основі яких формуються кластери для вирішення питання підготовки IT-кадрів» [13, с. 76].

З метою забезпечення інформаційної безпеки необхідно створити національну систему інформаційної безпеки як формат співпраці державних органів, установ, організацій, приватного сектору, науково-дослідних установ та організацій, професійних асоціацій та неурядових організацій у сфері інформаційної безпеки.

Вбачається доцільним вирішення таких актуальних питань:

Розробити засадничий документ із регулювання інформаційного простору – Концепцію інформаційної політики України, в «якій передбачити засади, методи та засоби формування та провадження державної інформаційної політики» (зокрема щодо реалізації системи державної пропаганди, спрямованої як на внутрішнє, так і на зовнішнє інформаційне середовище; забезпечення достатнього рівня присутності якісного національного інформаційного продукту в українському та міжнародному інформаційному просторі тощо).

Оптимізувати державне управління інформаційною сферою у спосіб: – «утворення Національної ради України з питань комунікацій – конвергентного незалежного органу з регуляторними й наглядовими повноваженнями в інформаційній сфері (на базі Національної ради та НКРЗІ), до компетенції якої віднести регулювання діяльності у сфері телекомунікацій, користування радіочастотним ресурсом, телерадіомовлення, а також іншої діяльності, пов’язаної з використанням телекомунікаційної інфраструктури, зокрема в мережі Інтернет тощо»; «утворення Міністерства з комунікацій, інформації та інформатизації України – центрального органу виконавчої влади з провадження комплексної загальнодержавної інформаційної політики та політики в інформаційній сфері, передбачивши серед його повноважень, зокрема, формулювання та трансляції в українському суспільстві й назовні державних інформаційних пріоритетів, найважливіших повідомлень з базових аспектів життя держави, а

також координацію діяльності органів виконавчої влади щодо виконання загальнодержавних програм і проектів інформатизації тощо».

Унормувати діяльність в інформаційній сфері відповідно до міжнародних правових норм і сучасних викликів, зокрема у спосіб: «доопрацювання розробленого Міністерством юстиції України Проекту закону «Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності щодо засобів масової інформації», спрямованого на недопущення монополізації ЗМІ (в тому числі Інтернет-ЗМІ) та їх використання у маніпулятивних цілях»; «розроблення обов'язкового для виконання Кодексу етичної поведінки журналістів, найважливішим у якому має бути розділ «Відповідальність», що міститиме вказівку: хто, за що і як відповідає, порушуючи ту чи іншу етичну норму»; визначення у нормативно-правовому полі України таких понять, як «державна інформаційна політика», «інформаційно-психологічна безпека», «інформаційно-психологічні впливи» тощо.

Отже, проаналізувавши напрямки вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації, варто зауважити, щодеякі країни почали просувати проекти стратегій інформаційної безпеки, і Україна не є винятком. Система національної безпеки є багатокомпонентною, національна система інформаційної безпеки є її особливою підсистемою, метою якої є забезпечення функціонування та розвитку цієї системи. Забезпечення належного рівня інформаційної безпеки є необхідною умовою розвитку інформаційного суспільства. У дещо спрощеному вигляді під національною системою інформаційної безпеки пропонується розуміти сукупність специфічних для певної нації чи держави суб'єктів інформаційної безпеки, які взаємодіють з метою забезпечення незахищеності особи, суспільства та країни в цілому. Очевидною є потреба у створенні Національної системи інформаційної безпеки, коли цим займатимуться відповідні підрозділи Служби безпеки України, відповідні підрозділи Державної служби безпеки та Міністерства внутрішніх справ.

Координацію та ефективну взаємодію забезпечуватиме відповідний підрозділ РНБО. Одним із ключових питань організації ефективного функціонування національних систем інформаційної безпеки є налагодження взаємодії між компетентними державними органами, які є суб’єктами інформаційної безпеки, та координація такої діяльності.

ВИСНОВКИ

У магістерській роботі наведено вирішення актуального наукового завдання, що полягає в дослідженні публічного управління забезпеченням інформаційної безпеки в країнах Європейського союзу та США задля вдосконалення інформаційної безпеки України на основі адаптації їх досвіду. Отримані в процесі дослідження результати та практичні рекомендації свідчать про досягнення визначеної мети, виконання поставлених завдань та дають підстави для низки узагальнюючих висновків і пропозицій.

1. Розкрито поняття інформаційної безпеки. Зокрема, інформаційна безпека – це стан захищеності життєво важливих інтересів особи, суспільства та держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, що мінімізує шкоду, нанесену їм внаслідок: неповноти, своєчасності та недостовірності інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

Під національною системою інформаційної безпеки пропонується розуміти сукупність специфічних для певної нації чи держави суб'єктів інформаційної безпеки, які взаємодіють з метою забезпечення захищеності особи, суспільства та країни в цілому.

2. Охарактеризовано загальні принципи інформаційної безпеки, тобто її формування та функціонування. Основними принципами забезпечення інформаційної безпеки України є: «пріоритет прав людини»; «верховенство права»; «пріоритет договірних (мирних) засобів у вирішенні інформаційних конфліктів»; «адекватність заходів захисту національних інтересів України в інформаційній сфері реальним та потенційним загрозам»; «громадський контроль за діяльністю органів державної влади, що входять до системи забезпечення інформаційної безпеки України»; «додержання балансу інтересів особи, суспільства, держави, їх взаємна відповідальність»;

«чітке розмежування повноважень та функцій органів державної влади в системі забезпечення інформаційної безпеки України». Ми не претендуємо на вичерпність запропонованих принципів і вважаємо, що розвиток цивілізації, науково-технічного прогресу, глобалізація та загострення проблем, пов'язаних із безпекою життєдіяльності народів, неминуче вимагатимуть пошуку нових підходів до їх вирішення. Ми також вважаємо, що запропоновані принципи допоможуть уникнути фрагментації та формування національної системи інформаційної безпеки. Ці принципи забезпечення інформаційної безпеки є основою формування та функціонування системи інформаційної безпеки як системоутворюючого чинника всіх складових національної безпеки, норм і правил поведінки громадян, державних і громадських інститутів України у цій сфері.

3. Проаналізовано нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині. В цих країнах вважають вирішення проблеми інформаційної безпеки особистості, суспільства, держави, їх захисту від внутрішніх і зовнішніх, у тому числі гібридних загроз - одним із найважливіших стратегічних пріоритетів національної безпеки. Проблеми інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині посідають одне з провідних місць у пріоритетах державної політики та стратегій національної безпеки і зосереджуються на стандартах ЄС та НАТО. Таким чином, аналіз зарубіжного досвіду правового регулювання інформаційної безпеки показує не лише загальні тенденції, а й різні підходи до правового регулювання інформаційної безпеки. Нормативно-правове правове регулювання забезпечення інформаційної безпеки в країнах ЄС визначає основні напрямки європейської політики інформаційної безпеки: створення європейської системи попередження та інформування про нові загрози, правового забезпечення, пріоритетами якої є захист персональних даних, регулювання телекомунікаційних послуг та боротьба з кіберзлочинністю, посилення інформаційної безпеки на державному рівні шляхом впровадження ефективних та сумісних засобів інформаційної

безпеки та заохочення використання державами-членами електронних підписів під час надання державних онлайн-послуг тощо.

4. Здійснено аналіз забезпечення інформаційної безпеки в органах публічної влади США й розкрито основні їх особливості. Сполучені Штати у своїй політиці захисту інформації виходять з того, що перехоплення іноземними державами відкритої інформації, яка циркулює в державних і комерційних телекомунікаційних мережах, може завдати шкоди державі, оскільки обробка цієї інформації, порівняння та агрегування різнорідної інформації може призвести до розкриття державна інформація. секрети. Сполучені Штати забезпечують свою інформаційну безпеку, запобігаючи діям потенційного супротивника. Завдяки технологічній перевазі США країна може отримувати, обробляти та використовувати інформацію, не даючи ворогові робити подібні дії. Це дозволяє Сполученим Штатам досягти військової переваги у невоєнний час. Аналіз законодавства США у сфері інформаційної безпеки показує, що основними напрямами забезпечення національної кібербезпеки США є захист критично важливих об'єктів інфраструктури, а саме – «їх інформаційних систем від кібернетичних атак»; «вдосконалення засобів виявлення таких атак і оперативного реагування на них»; «визначення завдань безпеки кіберпростору та способи їх вирішення»; «підготовка відповідних фахівців з безпеки інформації та взаємодія з приватним сектором»; «співпраця з міжнародними організаціями з метою забезпечення відкритого, безпечного, надійного кіберпростору».

Забезпечення інформаційної безпеки в органах публічної влади США, існують чітко визначені проблеми та виклики, з якими Сполученим Штатам постійно доводиться стикатися, як всередині держави, так і за її межами. Основним завданням уряду в таких умовах має стати розробка та вироблення єдиного бачення державної політики у сфері інформаційної безпеки з формуванням потужної системи захисту та постійним удосконаленням останньої для протидії зовнішнім і внутрішнім загрозам. Такі кроки дозволять запобігти інформаційним атакам та когнітивному зовнішньому

впливу на громадськість у майбутньому за умови консенсусу серед основних політичних сил США. Крім того, зосередженість урядових, корпоративних і громадських акторів на подоланні спільної проблеми позитивно вплине на загальний стан справ у Сполучених Штатах.

5. Визначені основні напрями вдосконалення забезпечення інформаційної безпеки через адаптацію кращого зарубіжного досвіду та удосконалення організації доступу до публічної інформації. Сьогодні не існує універсального підходу чи єдиної моделі управління інформаційною безпекою. Кожен регіон світу і країни мають свої внутрішні особливості, які згодом визначають специфіку цього процесу.

Системи інформаційної безпеки Франції та Німеччини ґрунтуються на усвідомленні ризиків і загроз, які несе стрімкий розвиток інформаційно-комунікаційних технологій. Тому політика цих країн у цій сфері є послідовною, заснованою на компетентних оцінках та стратегіях, спрямованих на навчання та розвиток технологій. Наприклад, одним з головних дійових осіб у системі інформаційної безпеки Франції є Національне агентство безпеки інформаційних систем (ANSSI), а в Німеччині — Відділ операцій з інформаційними та комп'ютерними мережами Бундесверу. Основними тенденціями їх роботи є технологічне лідерство та міжнародне співробітництво. Деякі країни почали просувати проекти стратегій інформаційної безпеки, і Україна не є винятком. Система національної безпеки є багатокомпонентною, національна система інформаційної безпеки є її особливою підсистемою, метою якої є забезпечення функціонування та розвитку цієї системи.

Забезпечення належного рівня інформаційної безпеки в Україні є необхідною умовою розвитку інформаційного суспільства. Очевидною є потреба у створенні Національної системи інформаційної безпеки, коли цим займатимуться відповідні підрозділи Служби безпеки України, відповідні підрозділи Державної служби безпеки та Міністерства внутрішніх справ. Координацію та ефективну взаємодію забезпечуватиме відповідний підрозділ

РНБО. Одним із ключових питань організації ефективного функціонування національних систем інформаційної безпеки є налагодження взаємодії між компетентними державними органами, які є суб'єктами інформаційної безпеки, та координація такої діяльності.

Шляхи досягнення інформаційної безпеки в Україні пов'язані із створенням безпечного інформаційного простору, що має включати: «наявність чіткої законодавчо-нормативної бази, що регулює відносини у сфері функціонування інформації, в тому числі й систему покарань за дезінформацію та способи протидії маніпулюванню свідомістю (суттєвим зрушенням тут є прийняття Доктрини інформаційної безпеки України)»; «сприяння державою до масового розповсюдження сучасних інформаційно-комунікативних технологій, впровадженню новітніх стандартів та розробок»; підвищення рівня інформаційної грамотності громадян (можливо, шляхом створення серії вебінарів, запровадження спеціальних майстер-класів тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакіна-Пілявська Л. М. Кримінально-правова охорона інформаційної безпеки: виклики сьогодення. *Актуальні проблеми протидії корупції 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. Є. Питання формування організаційної структури системи управління інформаційною безпекою підприємства. *Сучасний захист інформації*. 2016. № 1. С. 79–83.
3. Андрощук Р. В., Москаленко Р. В. Управління інформаційною безпекою військових формувань : 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 наук з державного управління. 25.00.02. Механізми державного управління. Національна академія державного управління при Президентові України. Київ. 2017. 218 с.
5. Апетик А. Інформаційна безпека. 2019. URL: https://www.prostir.ua/%3Flibrary%3Dinformatsijnabezpeka-now-yakyh-elementiv-ne-vystachaje+&cd=3&hl =ru&ct=clnk&gl=ua (дата звернення: 9.11.2023).
6. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики: монографія. Х.: Нац. ун-т внутр. оправ, 2006. 354 с.
7. Артемов В. Ю. Управління інформаційною безпекою як сутнісна складова побудови інформаційного суспільства в Україні : thesis. 2009. URL: http://essuir.sumdu.edu.ua/handle/123456789/11939 (дата звернення: 9.11.2023).
8. Бакалинський О. О. Модель та методи визначення проектних характеристик систем управління інформаційною безпекою : автореф.

дис. … канд. техн. наук. Київ, 2019. 19 с.

9. Безштанько В. Цикл впровадження системи управління інформаційною безпекою. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. Вип. 2 (13). С. 123–126.
10. Березовська І. Р. Суб'єкти у сфері забезпечення інформаційної безпеки в Україні. Наукові записки Львівського університету бізнесу та права. 2013. Вип. 10. С. 148-153.
11. Богуш В.М., Юдін О.К. Інформаційна безпека держави. К. : МК-Прес, 2005. 432 с.
12. Бондаренко Н., Ситниченко О. Організаційно-правове забезпечення інформаційної безпеки підприємств. *Foreign trade: economics, finance, law*. 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. Державне стратегічне управління: сутність та механізми його реалізації. *Економіка та держава.* 2011. № 1. С. 121-125.
14. Бурило Ю. П. Правові форми державного управління інформаційною сферою. *Юриспруденція: теорія і практика*. 2007. № 8. С. 2–10.
15. Бурич К. Л. Інформаційна безпека України у сучасному кіберпросторі. *Національна безпека і оборона.* 2014. №10. С. 21-27.
16. Варенья Н. М. Щодо методів виявлення небезпек та загроз терористичного характеру. *Верховенство права у процесі державотворення та захисту прав людини в Україні*: тези міжнародної наук.-практ. конф. (Одеса, 12-13 лютого 2016 року). Одеса: ГО «Причорноморська фундація права», 2016. С. 104-108.
17. Вербицька А.М., Дзюба Т.М., Кацалап В.О. Кіберскладова гібридної війни проти України. *Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017р.* Маріуполь: ДонДУУ. 2017. С. 255-258.
18. Воробйова І. В. Інформаційно-психологічна зброя як самостійний засіб

ведення інформаційно-психологічної війни. *Системи озброєння і військова техніка.* 2010. № 1. С. 141-144.

19. Герасименко К.С. Сучасні ознаки загроз «інформаційного тероризму». *Форум права.* 2009. № 3. С. 162-166.
20. Гібридна війна: in verbo et in praxi: монографія. Донецький національний університет імені Василя Стуса. Під. заг. ред. проф. Р.О. Додонова. Вінниця: ТОВ «Нілан-ЛТД». 2017. 412 с.
21. Головка А.А. Діяльність сучасних ЗМІ в контексті інформаційної безпеки України. *Актуальні проблеми гуманітарних та природничих наук* (м. Ужгород, 08-09 квітня 2016 р.). Херсон: Видавничий дім «Гельветика», 2016. С. 85-87.
22. Гончаров М. В. Досвід нормативно-правового забезпечення інформаційної безпеки 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 В.П., Биченок М.М., Копка П.М. Актуальні проблеми системного забезпечення інформаційної безпеки України : матеріали міжар. наук.- практ. конф. *«Форми та методи забезпечення інформаційної безпеки держави».* К.: Нац. Акад. СБ України. 2008. С. 79-85.
24. Горова С. В. Особа в інформаційному суспільстві: виклики сьогодення : монографія / наук. ред. О. С. Онищенко ; НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ, 2017. 342 с.
25. Григор'єв В.І. Інформаційна безпека у державному управлінні. *Бібліотекознавство. Документознавство. Інформологія.* 2013. № 4. С. 53-55.
26. Гурковський В. І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика) : монографія. Київ: Наук. світ, 2010. 396 с.
27. Дем’янюк Ю. Організаційно-педагогічні умови підготовки офіцерів-

прикордонників у магістратурі щодо управління інформаційною безпекою. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: педагогічні науки*. 2020. Т. 19, № 4. С. 147–160. URL: https://doi.org/10.32453/pedzbirnyk.v19i4.263 (дата звернення: 9.11.2023).

28. Дідківська Г. В., Топчій В. В. Криміналістичні механізми охорони інформаційної безпеки. *Ірпінський юридичний часопис*. 2023. № 3(12). С. 236–242. URL: https://doi.org/10.33244/2617-4154-3(12)-2023-236-242 (дата звернення: 9.11.2023).
29. Домарєв Д. В. Метод інформаційно-аналітичної підтримки управління інформаційною безпекою на основі структуризації оцінок : автореф. дис. … канд. техн. наук. Київ, 2015. 20 с.
30. Дотримання інформаційних прав і свобод українських громадян: нормативно-правове забезпечення і регулятивні важелі. Аналітична записка. URL: https://niss.gov.ua/dosHdzhennya/informaciyni-strategii/dotrimannya-informaciynikhprav- i-svobod-ukrainskikh-gromadyan (дата звернення: 9.11.2023).
31. Друцул Т. І. Заходи забезпечення національної безпеки органами публічної адміністрації. *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: 9.11.2023).
32. Думчиков М. О. Види органів державної влади у сфері забезпечення інформаційної безпеки та характеристика їх повноважень. *Європейські перспективи*. 2023. № 3. С. 222–227. URL: https://doi.org/10.32782/ep.2023.3.31 (дата звернення: 9.11.2023).
33. Економічне обгрунтування управління інформаційною безпекою підприємства : thesis / І. М. 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. *Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення:* матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017 р. Маріуполь: ДонДУУ. 2017. С.263-266.
35. Заплатинський В.М. Логіко-детермінантні 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 національний університет імені Івана Огієнка. 2012. Випуск 5. С. 90-98.
36. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків: ХНПУ. 2017. Вип.48 (частина І). С. 212-219.
37. Згуровський М. З. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. К., 2000. С. 10-14.
38. Зеленін В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни. Т. 1. Вінниця: Вид-во «Віндрук». 2014 . 384с.
39. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк». 2018. 446 с.
40. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки.* Вип. 2. № 1. 2016. С. 27-32.
41. Ісайко Д. Стратегія забезпечення національної безпеки в України. *Теоретичні та прикладні питання державотворення*. 2023. № 29. С. 199–201. URL: https://doi.org/10.35432/tisb292023289628 (дата звернення: 9.11.2023).
42. Іськів І. Підвищення ефективності державної політики у сфері

забезпечення економічної, соціальної та інформаційної складових національної безпеки. *Наукові перспективи (Naukovì perspektivi)*. 2023. № 7(37). URL: https://doi.org/10.52058/2708-7530-2023-7(37)-165-172 (дата звернення: 9.11.2023).

43. Іськів І. Характеристика сутності забезпечення національної безпеки. *Теоретичні та прикладні питання державотворення*. 2023. № 27. С. 143–147. URL: https://doi.org/10.35432/tisb272022276823 (дата звернення: 9.11.2023).
44. Кавин С. Нормативно-правове забезпечення інформаційної безпеки України в контексті набуття членства в європейському союзі. *Наше право*. 2023. № 3. С. 140–150. URL: https://doi.org/10.32782/np.2023.3.21 (дата звернення: 9.11.2023).
45. Кавин С. Я. Міжнародно-правове регулювання забезпечення інформаційної безпеки в рамках міжнародних організацій. *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 забезпечення інформаційної й інформаційно-психологічної безпеки. *Reports of the national academy of sciences of ukraine*. 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. *Grail of science*. 2023. № 27. С. 270–272. URL: https://doi.org/10.36074/grail-of-science.12.05.2023.042 (дата звернення: 9.11.2023).
48. Кириченко М. О. Формування ідеології інформаційного суспільства як фактор динамічного розвитку і безпеки сучасної України в XXI столітті. *Вісник Львівського університету. Серія Філософсько-політологічні студії: збірник наукових праць.* 2017. № 12. С. 74-81.
49. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного

суспільства. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2023. № 3(63). С. 38–42. URL: https://doi.org/10.32689/2523-4625-2022-3(63)-6 (дата звернення: 9.11.2023).

50. Коваль З. Проблематика протидії інформаційно-психологічним загрозам Україні засобами державного управління. електрон. наук. фах. вид. 2013. Вип. 13. URL: http://nbuv.gov.ua/j-pdf/tppd_2013_13_12.pdf (дата звернення: 9.11.2023).
51. Ковтун С.В. Інформаційна безпека: підручник. Харків. Вид. ХНЕУ, 2009. 368 с.
52. Коженьовські Л. Управління безпекою. *Актуальні проблеми економіки.* 2004. № 1 (31). С. 147-154.
53. Конституція України, Закон від 28.06.1996 № 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. Корєєва Н. Г. Формування сучасної системи управління інформаційною безпекою військової частини : thesis. 2020. URL: http://ir.stu.cn.ua/123456789/19964 (дата звернення: 9.11.2023).
55. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса: Юридична література, 2003. 472 с.
56. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України. Дис. ... д-ра юрид. наук : 12.00.07. Одеса. 2004. 427 с.
57. Котляров В. Основні підходи у концепції інформаційної безпеки. *Актуальні питання у сучасній науці*. 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 у контексті забезпечення національних інтересів. *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 засади сутності та концепції інформаційної безпеки. *Наукові перспективи (Naukovì perspektivi)*. 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-правова основа громадянського суспільства. *Право України,* 2015. № 4. С. 35-42.
61. Криволап Є., Юринець Ю. Взаємозв'язок безпекових стратегій України з інформаційною безпекою та кібербзпекою. *Актуальні питання у сучасній науці*. 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. *Відомості Верховної Ради України (ВВР)*. 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 9.11.2023).
63. Крупнова А. О. Перспективи правового регулювання інформаційної безпеки України. *Актуальні проблеми протидії корупції 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 у забезпеченні національної безпеки України. *Актуальні питання у сучасній науці*. 2023. № 10(16). URL: https://doi.org/10.52058/2786-6300-2023-10(16)-227-239 (дата звернення: 9.11.2023).
65. Кульчій О. О. Правове регулювання державної політики у сфері мас-медіа України. *Форум права.* 2015. № 3. С. 131-134.
66. Кустовська О. В. Методологія системного підходу та наукових досліджень: Курс лекцій. Тернопіль: Економічна думка, 2005. 124 с.
67. Лазарів В. Концептуальні засади пубулічного управління інформаційною безпекою електронних послуг: теорія та виклики. *Наукові перспективи (Naukovì perspektivi)*. 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 національної безпеки. *Kyiv law journal*. 2023. № 4. С. 83–88. URL: https://doi.org/10.32782/klj/2022.4.12 (дата звернення: 9.11.2023).
69. Леоненко Н. А. Зарубіжний досвід правового регулювання забезпечення національної безпеки. *Bulletin of the national university of civil protection of ukraine. series: public administration*. 2023. № 1(18)2023. URL: https://doi.org/10.52363/2414-5866-2023-1-14 (дата звернення: 9.11.2023).
70. Литовченко І. В. Основні тенденції інституціоналізації інформаційно-комунікаційного середовища сучасного суспільства. *Вісник Національного авіаційного університету. Сер. Соціологія. Політологія* : зб. наук. праць. Київ: НАУ, 2014. Вип. 1. С. 30-34.
71. Лихова С. Я., Пацеля Г. А. Колаборaційна діяльність у сфері інформаційної безпеки. *Права людини та публічне врядування 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: навчальний посібник. Київ: КНТ. 2009. 576 с. 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 умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.
74. Лук'янченко О. О. Економіко-організаційне забезпечення розвитку комунальної місто обслуговуючої сфери. Донецьк, 2008 р. 367 с.
75. Луцький М. Медіаосвіта як чинник інформаційної безпеки України. *Scientific works of national aviation university. series: law journal "air and space law"*. 2023. Т. 1, № 66. С. 206–213. URL: https://doi.org/10.18372/2307-9061.66.17438 (дата звернення: 9.11.2023).
76. Лянной Ю. О. Визначення видів реабілітації у професійній підготовці майбутніх магістрів з фізичної реабілітації. Вісник Чернігівського національного педагогічного університету. Сер.: Педагогічні науки.

Фізичне виховання та спорт. 2013. Вип. 112(2). С. 177-182.

77. Ляхович Г. І. Щодо сучасного розуміння сутності та особливостей державного управління в державі. *ВісникХНУВС.* 2009. № 3 (46). С. 129-136.
78. Магула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці. 03.07.2014. URL: https://naub.oa.edu.ua/2014/fenomen- informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/ (дата обращения: 08.07.2019).
79. Маковій В. П., Усата Г. О. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави. *Maritime security and defense*. 2023. № 1. С. 62-68. URL: https://doi.org/10.32782/msd/2023.1.8 (дата звернення: 9.11.2023).
80. Малик Я. Й., Береза О. І. Забезпечення інформаційної безпеки України у контексті світового досвіду. *Ефективність державного управління.* 2012. Вип. 32. С. 20-27.
81. Мамонов І. Потреби та інтереси людини як основа публічного управління. *Вісник Національної академії державного управління при Президентові України.* 2012. Вип. 3. С. 212-220.
82. Марків О. Т. Постправда та фактчекінг – тренди сучасної комунікації. *Наука та освіта: ключові питання сучасності.* 2018. Т11. С 11-119.
83. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика.* 2010. № 3(27). С. 17-21.
84. Медвідь В. Ю., Правдивець О. М., Кривчун Р. Ю. Теоретико-методичні засади формування системи управління інформаційною безпекою підприємства. *Agrosvit*. 2023. № 1. С. 24-30. URL: https://doi.org/10.32702/2306-6792.2023.1.24 (дата звернення: 9.11.2023).
85. Мельничук О. В. 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/10.36030/2664-3618-2018-1-42-60 (дата звернення: 9.11.2023).

86. Мокій А. В. Дослідження методів обробки ризиків у системах управління інформаційною безпекою. 2018. 99 с. URL: https://ela.kpi.ua/handle/123456789/26820 (дата звернення: 9.11.2023).
87. Мохова Ю. Л., Луцька А. І. Сутність та головні напрямки державної інформаційної політики України. *Державне управління: удосконалення та розвиток* : електр. наук. фах. вид. / Дніпропетров. держ. аграр.-екон. ун-т. 2018. № 12. URL: http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf (дата звернення: 9.11.2023).
88. Мохор В., Цуркан В. Методологія побудови систем управління інформаційною безпекою. *Ukrainian information security research journal*. 2022. Т. 23, № 4. С. 200–211. URL: https://doi.org/10.18372/2410-7840.23.16766 (дата звернення: 9.11.2023).
89. Муравська (Якубівська) Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. *Економіка і суспільство.* 2017. Вип. № 9. С. 289-294.
90. Наконечний В. С. Стан розвитку управління інформаційною безпекою в світовій практиці та її вплив на економічний розвиток України. *Сучасний захист інформації*. 2015. № 4. С. 10–15.
91. Настюк В.Я, Бєлєвцева В.В Правовий захист інформаційних прав і свобод 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 звернення: 9.11.2023).
92. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
93. Нестеряк Ю. В. Законодавче врегулювання відносин влади і засобів

масової комунікації: принципи та механізми на основі узагальнення міжнародного досвіду. *Державне управління: теорія та практика* : електрон. наук. фах. вид. 2011. № 2. URL: http://academy.gov.ua/ej/ej14/txts/Nesteryak.pdf (дата звернення: 9.11.2023).

94. Норчук Ю. В. 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).
95. Овчаренко М. Центр оперативного управління інформаційною безпекою. *Advanced discoveries of modern science: experience, approaches and innovations* / chair O. Сєвєрінов. 2021. URL: https://doi.org/10.36074/logos-09.04.2021.v1.49 (дата звернення: 9.11.2023).
96. Овчаренко М. Ю., Сєвєрінов О. В. Аналіз правил кореляції в системах управління інформаційною безпекою та подіями безпеки : thesis. 2021. URL: https://openarchive.nure.ua/handle/document/15763 (дата звернення: 9.11.2023).
97. Овчаренко М. Ю., Сєвєрінов О. В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки : thesis. 2019. URL: https://openarchive.nure.ua/handle/document/15774 (дата звернення: 9.11.2023).
98. Олійник О. В. Адміністративні реформи та їх вплив на забезпечення інформаційної безпеки в Україні. *Наукові записки інституту законодавства верховної ради України*. 2012. № 4. С. 53–56.
99. Олійник О. В. Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи.* 2012. № 4(1). С. 65-68.
100. Олійник О. В. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України. *Наукові записки інституту законодавства верховної ради України*. 2015. № 1. С. 54–59.
101. Олійник О. В. Методологічні засади забезпечення системи

інформаційної безпеки та її складової - захисту інформаційних ресурсів. *Право і безпека*. 2014. № 1 (52). С. 103–108.

102. Олійник О. В. Правові аспекти оптимізації організаційних засад інформаційної безпеки. *Бюлетень міністерства юстиції України*. 2013. № 1 (135). С. 73–78.
103. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Наукові праці Національного авіаційного університету. Юридичний вісник "Повітряне і космічне право"*. 2016. № 4 (41). С. 72–78.
104. Опанасенко Я. О. Роль і місце організаційної, соціальної й інформаційної складових у реалізації державної регіональної політики в умовах невизначеності регіонів. *Вісник Національного університету цивільного захисту України (Серія: Державне управління),* 2016. № 1 (4). С. 203-209.
105. Опірський І. Р., Головчак Р. В., Мосійчук І. Р. Перспективи розвитку систем штучного інтелекту в контексті інформаційної безпеки. *Ukrainian scientific journal of information security*. 2023. Т. 26, № 2. С. 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 підприємств : thesis. 2017. URL: https://er.knutd.edu.ua/handle/123456789/8187 (дата звернення: 9.11.2023).
107. Панченко О. Турбулентні соціально-психологічні виклики в системі державного управління інформаційною безпекою. *Theory and practice of public administration*. 2020. Т. 1, № 68. С. 210–217. URL: https://doi.org/10.34213/tp.20.01.25 (дата звернення: 9.11.2023).
108. Панченко О. А, Сердюк І. А. Роль держави в особистісних та суспільних відносинах в епоху турбулентності. Материалы Международной научно-практической интернет-конференции *«Тенденции и перспективы развития науки и образования в условиях глобализации». (28 февраля 2020 г.)* Переяслав - 2020. Вып. 56. С. 42-45.
109. Пічура В. Ю. Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів : бакалаврська

робота. 2021. URL: http://elar.khnu.km.ua/jspui/handle/123456789/10388 (дата звернення: 9.11.2023).

110. Про інформацію: Закон України від 02.10.1992 року № 2658-XII [Редакція від 03.12.2019 р.]. 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 № 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 09.01.2007 № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16#Text
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 грудня 2005 року № 3160. Відомості Верховної Ради України. 2006. № 8. С. 231. Ст. 94.
117. Про судоустрій і статус суддів: Закон України від 26.04.01 р. № 2402-III. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text (Редакція від 20.06.2020) (дата звернення: 9.11.2023)
118. Редзюк В., Редзюк Н. Сучасні проблеми інформаційної безпеки України та напрями їх вирішення. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2023. № 3. С. 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 і 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). С. 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 питання у сучасній науці*. 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 та 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 інформаційної безпеки особистості. *VII Міжнародна науково-практична конференція «Психолого-педагогічні, правові та соціально-культурні 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. Й., Кудін С. В. Методологічні засади нормативно-правового забезпечення інформаційної безпеки. *Ірпінський юридичний часопис*. 2023. № 2(11). С. 48–55. URL: https://doi.org/10.33244/2617-4154-2(11)-2023-48-55 (дата звернення: 9.11.2023).
125. Шевченко В. Л. Кращі світові практики управління інформаційною безпекою та їх 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. *Society document communication*. 2023. № 19.

С. 270–286. URL: https://doi.org/10.31470/2518-7600-2023-19-270-286 (дата звернення: 9.11.2023).

127. Шульга О. А. Управління рекламно-інформаційною діяльністю підприємства. *Підприємництво і торгівля*. 2023. № 38. С. 84–93. URL: https://doi.org/10.32782/2522-1256-2023-38-11 (дата звернення: 9.11.2023).

128. Arkhypov O., Teplytska T. Adaptive approach to information security management. *Young scientist*. 2019. Vol. 11, no. 75. URL: https://doi.org/10.32839/2304-5809/2019-11-75-142 (date of access: 9.11.2023).

129. Bratsuk I., Kavyn S. International legal regulation of ensuring information security within the framework of the un. *Bulletin of taras shevchenko national university of kyiv. legal studies*. 2023. No. 125. P. 21–26. URL: https://doi.org/10.17721/1728-2195/2023/1.125-4 (date of access: 09.11.2023).

130. Nesen M., Liashevska V., Fomina Y. Management of information security of production. *Economics: time realities*. 2021. Vol. 2, no. 54. P. 39–46. URL: https://doi.org/10.15276/etr.02.2021.5 (date of access: 17.12.2023).