ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра публічногоуправління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на тему: ***«Публічне управління забезпеченням інформаційної безпеки: досвід країн ЄС та США для України»***

Виконала: студентка магістратури
заспеціальністю
281 Публічнеуправління та
адміністрування
Тимощук Анна Ростиславівна

Керівник: кандидатка наук з
державногоуправління, доцентка
Гаман Тетяна Василівна

Рецензент:

Хмельницький – 2021 рік

ЗМІСТ

АНОТАЦІЯ

Тимощук А.Р. Публічне управління забезпеченням інформаційної безпеки: досвід країн ЄС та США для України

У магістерській роботі висвітлено основні засади публічного управління забезпечення інформаційної безпеки. Зокрема, охарактеризовано сутність інформаційної безпеки, історію виникнення та основні принципи забезпечення інформаційної безпеки.

Проаналізовано нормативно-правове регулювання інформаційної безпеки в окремих країнах Європи та США. Розглянуто базові закони, якими регулюється забезпечення інформаційної безпеки щодо. Зокрема, висвітлено особливості забезпечення інформаційної безпеки в органах публічної влади США, Німеччини, Польщі, Хорватії, Угорщини та Франції. Охарактеризовано діяльність зазначених країн щодо забезпечення інформаційної безпеки. На підставі досвіду країн ЄС та США, нами розроблені напрями вдосконалення забезпечення інформаційної безпеки нашої держави через адаптацію кращого досвіду досліджуваних країн та визначення напрямів удосконалення організації доступу до публічної інформації в Україні.

Ключові слова: інформаційна безпека, принципи, нормативно-правове регулювання інформаційної безпеки, органи публічної влади, публічна інформація.

ANNOTATION

Tymoshchuk A.R. Public management of information security: the experience of the EU and the USA for Ukraine

The master's thesis highlights the basic principles of public administration of information security. In particular, the essence of information security, history of origin and basic principles of information security are described.

The normative-legal regulation of information security in separate European countries is analyzed. The main laws governing the country on information security are considered. In particular, the peculiarities of information security in the public authorities of the United States, Germany, Poland, Croatia, Hungary and France are highlighted. The systems of these countries to ensure information security are described. Based on the experience of the United States and the EU, we have developed ways to improve information security and access to public information in Ukraine.

Key words: information security, principles, normative-legal regulation of information security, public authorities, public information.

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: А.А.Баранов [5], В.О. Бондаренко [6], М. О. Кельман [11], О.О. Климчук [12], З.В. Коваль [13], В. К. Колпаков [14], Б. А. Кормич [16], А. Б. Логунов [17], Г.Ю. Маклаков [18], Р.Р. Марутян [19], Г.Г. Почепцов [21], А.А. Стрельцов [24], Л.В. Туманова [26], Ю.С. Уфимцев [27], В.П. Шеломенцев [28].

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 принципизабезпечення інформаційної безпеки;
- проаналізувати нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині;
- здійснити аналіз забезпечення інформаційної безпеки в органах публічної влади 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 дослідженняможе бути використанеу 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, висновківта 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 відповідно до Постанови ЦК КПРС та Ради Міністрів СРСР № 903-303 від 18 грудня 1973 р. За період існування Комісії було створено потужну систему органів захисту інформації та забезпечення ІБ» [31].

8 грудня 1991 р. Головою Верховної Ради Білорусі, президентами України та Російської Федерації 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., на підставі Рішення про Програму розвитку військового співробітництва держав-учасниць СНД до 2001 р., було затверджено Концепцію інформаційної безпеки держав-учасниць СНД у військовій сфері, яку підписали Республіка Вірменія, Республіка Білорусь, Республіка Казахстан, Киргизська Республіка, Російська Федерація та Республіка 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].

У 2005 р. на двадцять шостому пленарному засіданні Міжпарламентської асамблеї держав-учасниць СНД вперше «було прийнято Модельний закон про інформатизацію, інформацію та захист інформації. 10

жовтня 2008 р. у м. Бішкек Рішенням Ради голів держав СНД було затверджено Концепцію співробітництва держав-учасниць СНД у сфері гарантування інформаційної безпеки одночасно з Комплексним планом заходів щодо її реалізації на період 2008-2010 рр. 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 України від 8 липня 2009 р. №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 – стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації, запропонувавши це визначення до широкого обговорення» [6, с. 78].

Таблиця 1.1.Характеристика поняття «інформаційна безпека» різними вченими

Автор	Характеристика поняття
Р.А. Калюжного	«Інформаційна безпека − це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації»
Б.А. Кормич	«Інформаційна безпека – це стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин»
О.Л. Морозов	«Інформаційна безпека держави є таким станом інститутів держави і суспільства, за якого забезпечується надійний захист національних інтересів країни і її громадян в інформаційній сфері»
В.А. Ліпкана	«Інформаційна безпека − це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України»
Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус	«Поняття інформаційної безпеки визначають виходячи з найімовірніших загроз національній безпеці України в життєво важливих сферах діяльності. Зокрема, під інформаційною безпекою, науковці розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни»

Примітка: власна розробка автора

Але наскільки це запропоноване визначення відповідає його сутності та відповідає суті поняття «інформаційний простір», спробуємо розібратися детальніше.

Для розуміння спрямованості простору, якій розглядається, слід згадати, що означає поняття «кібернетика», похідною якого є «кібернетичний». Кібернетика – «наука про управління, зв'язки і переробку інформації. Основний об`єкт дослідження – так звані кібернетичні системи, що розглядаються абстрактно, незалежно від їх матеріальної природи. Приклади кібернетичних систем – автоматичні регулятори у техніці, ЕОМ, людський мозок, біологічні популяції, людське суспільство. Кожна така

система є множиною взаємопов'язаних об'єктів (елементів системи), здатних сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею» [23, с. 456].

Виходячи з вищесказаного, можна зробити висновок «інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією».

Інформаційний простір має наступні властивості:

– «протяжність»;
– «єдність дискретності та неперервності»;
– «матеріальність та нематеріальність»;
– «абстрактність і дійсність»;
– «реальність загально-діючого впливу» [28, с. 314].

Рисунок 1.1 Властивості інформаційного простору

Примітка: побудоване автором на основі джерела [28]

Інформаційний простір має свою розмірність/довжину, яка визначається кількістю наявних матеріальних і нематеріальних об'єктів за певний період часу. У той час як довжина кіберпростору обмежена поверхнею земної кулі з точки зору наявності матеріальних об'єктів,

довжина інформаційного простору практично необмежена з точки зору наявності нематеріальних об’єктів.

Інформаційний простір включає і те і «матеріальну складову, наприклад, засоби обчислювальної техніки, засоби зв`язку, матеріальні складові телекомунікаційних мереж, написання алгоритмів і кодів та ін., так нематеріальну – інформацію, процеси зчитування кодів, процеси передачі інформації та ін. Але при цьому необхідно зауважити, що під матеріальністю, у даному випадку, ми розуміємо, на відміну від філософського розуміння, все те, що можна побачити, відчути або доторкнутися».

Отже, інформаційний простір є рукотворним продуктом людини, який вона сформувала для себе і для себе для задоволення своїх потреб, не замислюючись про «побічні» явища, про які йтиметься далі.

Саме це і вищесказане дають підстави стверджувати, що:

- «об’єктами інформаційного простору є живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею, серед яких, в першу чергу, людина, визначені верстви суспільства та суспільство в цілому, держава, природні та штучні інформаційні відносини між ними та їх формування і використання, а також матеріальні та нематеріальні об`єкти і процеси, спрямовані на породження, сприйняття, запам`ятовування, збереження, переробку та обмін інформацією»;

- «суб’єктами кіберпростору є людина, суспільство, держава, а також жива істота, яка спроможна сприймати, запам`ятовувати та переробляти інформацію, а також обмінюватися нею» [28, с.315].

Але для подальших досліджень по визначенню поняття «інформаційна безпека» напрошується необхідність визначення відмінностей у поняттях «інформаційний простір» та «кіберпростір».

Інформаційний простір – це «форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі» [28, с. 315].

Інформаційний простір – це «форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі».

Перш за все, слід розуміти, що за цим визначенням інформаційна безпека – це«деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть діяти якісь загрози з кіберпростору, послуг інформаційних систем це визначення терміна дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий методологічний зміст у розумінні місця і ролі проблеми інформаційної безпеки в інших видах безпеки» [28, с. 316].

У німецькій стратегії під інформаційною безпекою розуміється комплекс необхідних і доцільних заходів, виконанням яких досягається мінімізація ризику. При цьому в стратегії зазначено, що інформаційна безпека має базуватися на комплексному підході. Це досить прагматична точка зору, яка дозволяє розробити практичні кроки щодо забезпечення інформаційної безпеки, але не дає достатньої методологічної бази для проектування та оцінки систем, що забезпечують цю безпеку. Про це побічно свідчить зміст десяти стратегічних напрямків у стратегії інформаційної безпеки, оголошених федеральним урядом Німеччини [48].

У Канаді стверджують, що з «метою забезпечення найсучаснішого використання інформаційного простору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають. У канадській стратегії інформаційної безпеки не міститься чіткого визначення того, що являє собою інформаційна безпека. Відповідно до цього документа під інформаційною безпекою можна розуміти захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак. З

іншого боку, надано досить докладне визначення кібератаки, а кібербезпека – це засіб захисту від цих загроз» [42].

У цілому канадська стратегія як і раніше розглядає основний збиток від реалізації кіберзагроз як шкоду, яку можуть мати системи життєзабезпечення та підтримувати діяльність всієї країни, бізнесу та окремих громадян.

Одна з найновіших національних стратегій інформаційної безпеки (Турецька Республіка) містить таке визначення: інформаційна безпека – «захист інформаційних систем, що входять до складу інформаційного простору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам. При цьому під кіберпростором розуміється середовище, що складається з інформаційних систем, розподілених по всьому світу, в тому числі мереж, що з'єднують ці системи. Національний кіберпростір визначається як простір, який складається з інформаційних систем суб'єктів, що перебувають під юрисдикцією Турецької Республіки» [60].

Нідерланди також приділяють пильну увагу загрозі інформаційній інфраструктурі в контексті широкого використання цифрових (комп'ютерних) технологій. У 2013 році Національний координатор з питань безпеки та боротьби з тероризмом опублікував Національну стратегію інформаційної безпеки. На думку авторів стратегії, інформаційної безпека – це «сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз» [33].

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

Метою політики інформаційної безпеки уряду Австралії є «підтримка безпечної, стійкої і надійної роботи електронного операційного середовища,

яке підтримує національну безпеку Австралії та максимізує переваги цифрової економіки. В опублікованій у 2009 році Стратегії під інформаційною безпекою розуміється забезпечення доступності, цілісності та конфіденційності ІКТ Австралії, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання ІКТ для цілей сексуальної експлуатації» [49].

Український законопроект пропонує власний варіант визначення інформаційної безпеки, який розуміється«стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі. При цьому в законопроекті кіберпростір – середа, яка виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Дане визначення має дуже низький методологічний потенціал і не дозволяє конкретизувати особливості інформаційної безпеки. Більше того, абсолютно необґрунтовано до інформаційної безпеки віднесені проблеми функціонування інформаційних систем в загальному сенсі, внаслідок чого до проблематики інформаційної безпеки можуть бути віднесені телебачення і радіо, а також навіть бібліотеки та архіви» [3].

Враховуючи те, що проблема інформаційної безпеки має глобальний характер, позиція міжнародних організацій виглядає дуже цікавою. Так, Міжнародний союз електрозв'язку визначає у своїй Рекомендації наступне: інформаційна безпека — це сукупність інструментів, стратегій, принципів безпеки, гарантій безпеки, настанов, підходів до управління ризиками, дій, навчання, практичного досвіду, страхування та технологій, які можуть бути використовується для захисту інформаційного середовища, ресурсів організації та користувача.

При цьому ресурси організації та користувача включають «під’єднані комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи телекомунікацій і всю сукупність переданої та/або збереженої інформації в

інформаційному середовищі, а мета інформаційної безпеки полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в інформаційному середовищі. Загальні завдання забезпечення безпеки включають таке: доступність; цілісність, яка може включати автентичність і безвідмовність; конфіденційність» [22, с. 24].

Питання управління інформацією є елементом національної безпеки, державної безпеки.

Виходячи з наведеного, визначення, які надані у роботі, що «інформаційна безпека – стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації та у роботі– інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через» [42]:

– «негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації»;

– «негативні наслідки застосування інформаційних технологій»;

– «несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням, є справедливими» [42].

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства в основному визначається кількістю інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, якісно змінюється, зростає кількість її джерел і споживачів. Водночас зростає вразливість сучасного інформаційного суспільства перед недостовірною (а часом і шкідливою) інформацією, її несвоєчасним отриманням, промисловим шпигунством, комп’ютерною злочинністю тощо. Тому Конституція України вважає інформаційну безпеку однією з найважливіших функцій держави [4].

За даними наукових досліджень, «система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в межах адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів державної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки країни та інші чинники обумовлюють ескалацію загроз, що може призвести (а часом і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру, завдання шкоди юридичним особам та громадянам» [8, с. 90].

З огляду на викладене, варто зосередити увагу на одному з найважливіших аспектів забезпечення належного захисту інформаційної безпеки – координації діяльності органів державної влади, приватного сектору, громадських організацій та окремих осіб. Згідно зі ст.17 Конституції України, забезпечення інформаційної безпеки – це «справа усього українського народу. Проблема координації є важливою сама по собі та набуває значення у зв’язку з тим, що, на відміну від багатьох інших галузей, у сфері інформаційних технологій постійно змінюється термінологія, «ламаються» традиційні уявлення про методи та засоби передачі, отримання, обробки та зберігання інформації. Хоча часом за зміною вже сталих термінів простежується лише робота маркетологів щодо просування власних проектів. Це призводить до того, що одне й те саме поняття описується завдяки різним термінам, і навпаки – один і той самий термін несе різне значеннєве навантаження» [1].

Проблему інформаційної безпеки неможливо вирішити без впровадження нових ідей, нових знань, нової політики у сфері інформатизації. Концептуальними є пропозиції щодо широкого залучення вітчизняних науковців та виробників до її вирішення як складової національної безпеки. Вітчизняні спеціалісти повинні гарантувати високу якість інформаційних послуг, безпеку інформаційних технологій, сучасну

систему сертифікації програмно-технічних засобів, впровадження стандартизації, створення національних баз даних, телекомунікаційних систем, безпеку роботи у світовому інформаційному просторі.

Ігнорування цих проблем може призвести до труднощів у прийнятті найважливіших політичних, економічних, соціальних, військових рішень тощо.

Активно впливає рівень інформаційної безпеки на «стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз – це завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо» [18, с. 129].

На жаль, сьогодні в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації має стихійний, неконтрольований характер, з переважним ухилом до використання засобів інформатизації іноземного виробництва.

Отже, охарактеризувавши поняття, сутність, історія виникнення проблеми забезпеченням інформаційної безпеки, варто зауважити, що після радянських країн, як і в Україні, розвиток науково-дослідних напрямів забезпечення інформаційної безпеки людини та суспільства загалом почався лише в останнє десятиліття XX ст. і пов'язаний з початком демократичних реформ, пов'язаних із утвердженням державної незалежності та самостійності. 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.

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».

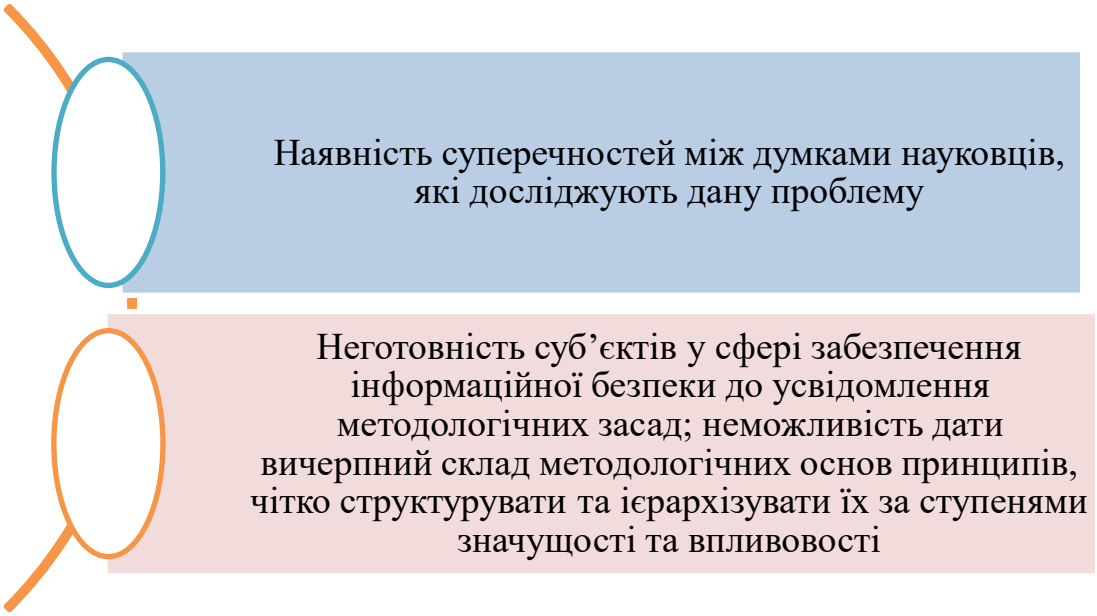

Рисунок 1.2 Основні причини проблеми визначення методологічних засад управління забезпеченням інформаційної безпеки

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. Обґрунтування певної системи принципів управління забезпеченням інформаційної безпеки означає підвищення методологічного рівня організаційної адекватності інформаційної безпеки соціально-економічному станові держави. Ґрунтуючись 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].

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].

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 управління	«нормативність діяльності, єдиноначальність, колегіальність, поділ управлінської праці; відповідальність за прийняті рішення; оперативна самостійність»

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

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:

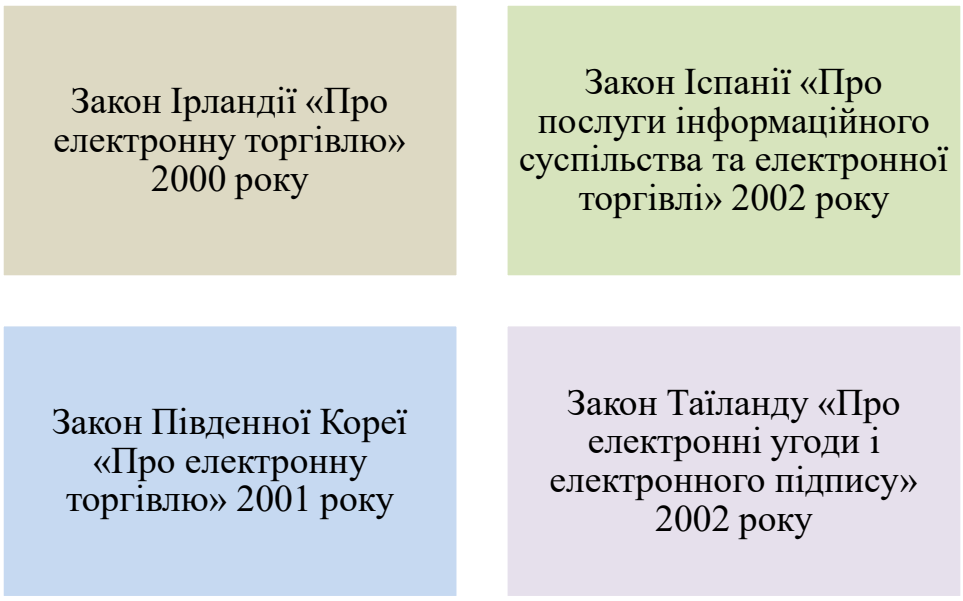

Рисунок 2.1 Набір законів і нормативних актів у сфері інформаційної безпеки в зарубіжних країнах

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: європейський політичний підхід», в якому «окреслено сучасний підхід ЄС до проблеми інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи» [44].

Документ визначає основні напрямки європейської політики інформаційної безпеки: «підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами»; «створення європейської системи попередження та інформування про нові загрози»; «забезпечення технологічної підтримки»; «підтримка ринково орієнтованої стандартизації та сертифікації»; «правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності»; «зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо»; «розвиток міжнародного співробітництва з питань інформаційної безпеки».

В ЄС також значна увага приділяється проблемі кібербезпеки як невід’ємної частини інформаційної безпеки. З 1999 року ЄС впроваджує програми «Безпечніший Інтернет», у рамках яких «здійснюються заходи, спрямовані не лише на боротьбу зі шкідливим контентом, але й з небезпечною поведінкою в мережі» [63].

У 2007 році Європейська комісія представила документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю», в якому «кіберзлочинність визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, і включає: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо)» [45].

У 2009 році було опубліковано повідомлення Європейської комісії під назвою «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості», в якому «визначено основні виклики/проблеми, які потребують негайного реагування з боку країн ЄС, а також окреслено основні заходи, необхідні для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам» [44].

Зокрема, в резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18 грудня 2013 року підкреслено глобальну і відкриту природу Інтернету і швидкий розвиток у сфері інформаційних та комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі підтверджено, що «ті ж права, що люди мають в офлайн-режимі, також повинні бути захищені онлайн, у тому числі право на приватність» [52].

Зокрема, це характерно для німецького законодавства «детальна розробка системи різних видів інформації з обмеженим доступом, чіткі формулювання їх визначень у федеральному законодавстві. Так, відповідно до Закону «Про перевірку безпеки» секретною інформацією є факти, вироби та відомості незалежно від форми їх представлення, які в державних інтересах повинні зберігатися в таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, котрий відповідає

необхідному рівню захисту [53].

У жовтні 1997 року в Німеччині був прийнятий Закон про захист телекомунікаційної інформації (TDPA). За її загальними принципами «збирання, обробка та використання інформації дозволяється лише у випадках, коли це дозволено законом або здійснюється за згодою користувача. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач, причому згода користувача не є умовою для надання послуг» [68].

При цьому з 2005 року в Німеччині діє «Акт про свободу інформації», який «регламентує питання доступу до інформації. Нагляд за виконанням положень цього нормативних акту покладений на комісара із захисту інформації та персональних даних. Починаючи з 1990 року в країні також діє закон про доступ приватних осіб і дослідників до архівів Штазі - колишньої Служби безпеки Східної Німеччини» [65].

Провідну роль у забезпеченні інформаційної безпеки Німеччини відіграє Федеральна служба інформаційної безпеки, як Закон Німеччини «Про посилення безпеки інформаційних систем» завдання щодо «попередження й реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема, у взаємодії із приватним сектором, покладається саме на це відомство. BSI входить до Федерального міністерства внутрішніх справ, яке, серед інших функцій, забезпечує внутрішню безпеку і захист конституційного ладу Німеччини, здійснює боротьбу з тероризмом, екстремізмом, шпигунством і саботажем. Відповідно до Закону «Про Федеральне відомство безпеки інформаційних систем» BSI збирає та оцінює інформацію стосовно загроз кібербезпеці держави, виявляє нові типи кібератак, аналізує відповідні контрзаходи» [40].

У співпраці з НАТО та ЄС, також покладені на такі функції: «оцінка ризику впровадження інформаційних технологій; розробка критеріїв, методів

і іспитових засобів для оцінки ступеня захищеності національних комунікаційних систем»; «перевірка ступеня захищеності інформаційних систем і видача відповідних сертифікатів»; «видача дозволів на впровадження інформаційних систем у важливі державні об'єкти»; «здійснення спеціальних заходів безпеки інформаційного обміну в державних органах, поліції тощо»; «консультування представників промисловості з питань інформаційної безпеки. Крім того, відомство займається пропагандою необхідності забезпечення інформаційної безпеки» [67].

З метою оптимізації оперативного співробітництва між усіма державними установами та покращення координації заходів протидії кібератакам у Німеччині на базі Федерального управління безпеки інформаційних систем, національного центру кіберзахисту (NCAZ), який «безпосередньо взаємодіє з іншими суб'єктами кібербезпеки країни, в тому числі з приватним сектором, країнами- партнерами з ЄС, НАТО, а також міжнародними організаціями» [67].

Федеральне бюро захисту конституції також відповідає за забезпечення інформаційної безпеки Німеччини в межах своєї компетенції (BFV) та Управління інформаційних операцій, «створене в 2009 року в структурі бундесверу через масовані атаки на обчислювальні мережі державних структур ФРН у лютому 2009 року» [74].

Також наприкінці 2010 року в рамках реалізації концепції кіберзахисту в структурі командування Бундесверу остаточно завершилося формування підрозділу інформаційно-комп'ютерних мережевих операцій, який функціонує з 5 квітня 2017 року як «Сили кібернетичного та інформаційного простору Німеччини». До завдань відповідного підрозділу входить, зокрема: «розробка нових методів кібератак; проникнення в комп'ютерні мережі іноземних держав і організацій з метою отримання розвідувальних даних; проведення операцій деструктивного впливу на мережі й автоматизовані системи або блокування їх роботи» [50].

Національна інформаційна політика Республіки Польщі «зорієнтована на побудову вільного відкритого суспільства, забезпечення прав людини, впровадження концепції вільного транскордонного обігу інформації, створення незалежних і плюралістичних мас-медіа». Її правовим підґрунтям є прийняті 90-х роках минулого століття «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща», в яких «визначаються напрями інформаційної політики, встановлюються технологічні стандарти інформаційного зв'язку, форми залучення іноземних інвестицій (від 33%- 49% зарубіжного капіталу), ліцензування інформаційної діяльності. Окремо визначаються права церкви на інформаційну діяльність, з огляду значного впливу клерикальної інформації на політичні пріоритети та моральність польського суспільства» [58].

Агентство внутрішньої безпеки відіграє ключову роль у забезпеченні кібербезпеки Польщі (ABW). У 2013 році ABW «розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій» [38].

ABW також «створило урядову команду реагування на комп'ютерні інциденти (CERT)»[47], головним завданням якої є «забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз, зокрема від атак на інфраструктуру, що складається з IT-систем та комп'ютерних мереж, порушення роботи або руйнація яких може значною мірою загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу або призвести до значних фінансових збитків і збоїв *у* функціонуванні органів державної влади» [12, с. 76].

Через ескалацію гібридних загроз інформаційного характеру, таких як пропаганда, дезінформація чи психологічне залякування з боку інших країн та недержавних акторів (терористичних та інших організацій) Управління національної безпеки Польщі (BBN)у 2015 році «розпочало роботу над

польською Доктриною інформаційної безпеки. Серед загроз інформаційній безпеці в Доктрині названі, зокрема, ескалація напруження в міжнародних стосунках, дискредитація польської міжнародної політики і формування негативного іміджу Польщі на міжнародній арені, в тому й серед союзників в рамках НАТО чи ЄС, формування образу Польщі як країни ксенофобів та антисемітів, провокування польсько-литовського конфлікту на тлі польської меншини у Литві, а також провокування польсько-українського конфлікту на історичному тлі при можливому застосуванні терористичних замахів, які буцімто могли б здійснити українці проти поляків чи навпаки» [35].

Якщо говорити про захист інформації з обмеженим доступом, то слід зазначити, що «при вступі до НАТО Польща, так само, як Чехія і Словаччина, розробила нове законодавство щодо захисту класифікованої інформації на підставі нових принципів». Так, у січні 1999 року набув чинності Закон «Про захист конфіденційної інформації», прийняття якого «було умовою вступу Польщі в НАТО. Закон поширюється на засекречену інформацію й дані, зібрані державними структурами», «розголошення яких може завдати шкоди державним або суспільним інтересам, або захищеним за законом інтересам громадян або організації» [58].

На відміну від Польщі, Угорщина адаптувала чинне законодавство НАТО для захисту державної та службової таємниці. Зокрема, «в 1995 році Угорщина прийняла закон про державні та офіційні секрети, який у 2001 році був доповнений і виправлений виходячи з практики Альянсу» [58].

Угорщина стала першою постсоціалістичною країною, яка «прийняла правовий акт про захист персональних даних - «Закон про захист інформації про особу та доступ до інформації, що становить суспільний інтерес» 1992 року, який впровадив інститут Парламентського комісара із захисту інформації та свободи інформації» [59].

Відповідно до цього Закону будь-яка інформація, що обробляється органами, які«виконують суспільні обов’язки, становить суспільний інтерес, за винятком інформації про особу. Проте доступ і поширення інформації про

діяльність політичних діячів і державних посадових осіб не можуть обмежуватися на підставі захисту інформації про особу. Закон також покладає на органи державної влади обов'язок надавати громадськості точну і своєчасну інформацію та надає право угорським громадянами звертатися із запитами про надання доступу до інформації, що становить суспільний інтерес. При цьому персональні дані можуть збиратися і оброблятися тільки з відома самої особи або відповідно до вимог закону».

Питання забезпечення інформаційної безпеки Угорщини, включаючи кібербезпеку, також охоплює Закон «Про електронну інформаційну безпеку державних та муніципальних органів» 2013 року [39] та п. 31 «Стратегії національної безпеки Угорщини», затвердженої у 2012 році [54].

Стратегія національної безпеки, зокрема, передбачає, що «Угорщина повинна бути готова управляти ризиками й загрозами, пов'язаними з інформаційною безпекою, обороною, боротьбою проти злочинності, а також запобігати нештатним ситуаціям у кіберпросторі, а також гарантувати адекватний рівень кібербезпеки й виконувати інші завдання, пов'язані із забезпеченням кібербезпеки. При цьому основним завданням визначається систематичне визначення пріоритетів усфері потенційних загроз і ризиків у кіберпросторі, а також підвищення поінформованості суспільства щодо них. Відповідні положення дістали свого подальшого розвитку у Національній стратегії кібербезпеки Угорщини, затвердженій у 2013 році» [61].

У Хорватії з 2007 року діє «Акт про інформаційну безпеку», що «визначає поняття інформаційної безпеки, заходи й стандарти інформаційної безпеки, а також сфери інформаційної безпеки та компетентні органи для прийняття й реалізації рішень у сфері забезпечення інформаційної безпеки, а також нагляду за дотриманням стандартів інформаційної безпеки. Зокрема, інформаційна безпека визначена як стан конфіденційності, цілісності й доступності інформації, що досягається шляхом реалізації політики заходів і стандартів і організаційної підтримки робочих місць, планування, реалізації, оцінки й відновлення заходів і стандартів» [55].

Крім того, у 2015 році Хорватія прийняла національну стратегію кібербезпеки. Стратегія кібербезпеки Хорватії ґрунтується на таких принципах:«всебічність підходу до кібербезпеки, що охоплює кіберпростір, інфраструктуру й користувачів відповідно до хорватської юрисдикції (громадянство, реєстрація, домен, адреса)»; «інтеграція заходів у різних сферах забезпечення інформаційної безпеки»; «зміцнення стійкості, надійності й керованості шляхом застосування універсальних критеріїв конфіденційності, цілісності й доступності певних груп інформації й соціальних цінностей»; «захист прав і свобод людини у кіберпросторі, передусім - конфіденційності та власності»; «постійне вдосконалення правової бази»; «субсидіарність при розподілі повноважень»; «пропорційність витрат на забезпечення кібербезпеки та ступеню ризику тощо» [69].

Отже, проаналізувавши нормативно-правове регулювання інформаційної безпеки в Німеччині, Польщі, Хорватії та Угорщині, варто зауважити, що нині європейські країни 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 особистості, суспільства, держави, їх захисту від різного роду загроз, як зовнішніх, так і внутрішніх, на сьогодні посідають одне з провідних місць у пріоритетах державної політики та стратегій національної безпеки Центральної Європи, які в цій питання зосереджені насамперед на стандартах ЄС та НАТО.

2.2 Характеристика забезпечення інформаційної безпеки в органах публічної влади (досвід США)

Аналізуючи забезпечення інформаційної безпеки в органах публічної

влади (досвід США), відзначимо, що «національна безпека США зазвичай визначається документом, який носить назву Стратегія національної безпеки США (NSS), розробляється окремо адміністрацією кожного нового президента та інтегрує зовнішню політику, національну оборону, міжнародні економічні відносини та політику допомоги у розвитку. Остаточно версія нової NSS побачила світ у грудні 2017 р. і виявилася однією з найдовших стратегій в історії США – принаймні, – майже вдвічі довшою, ніж попередня, опублікована у 2015 році» [72].

Абсолютно логічно навести, перш за все, досвід інформаційної безпеки, накопичений найвпливовішою в політичному, економічному та військовому відношенні державою – США.

З точки зору інформаційної безпеки США можна вважати першопрохідцем, оскільки це не лише перша країна у світі, яка запровадила електронне урядування з використанням новітніх інформаційних технологій, а й створила спеціальну систему захисту національного інформаційного суверенітету та безпеки. інформаційних ресурсів.

Звертаючись безпосередньо до характеристики системи американської моделі управління інформаційною безпекою, слід зазначити, що«у США функціонує кілька інституцій забезпечення інформаційної безпеки: Агентство національної безпеки (АНБ), Національне управління кібербезпеки міністерства внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР), Центральне розвідувальне управління (ЦРУ)» [72].

Варто зауважити, що «серед державних інституцій забезпечення інформаційної безпеки АНБ розвиває також партнерство з приватним сектором і науковими установами у вигляді планування заходів протидії загрозам у неурядових комп‘ютерних мережах (таким чином держава бере участь у захисті найважливіших приватних телекомунікаційних, електричних, банківських мереж (телекомунікації, електромережі, мережі банківських розрахунків, інтернет-провайдери). АНБ залучає до проведення заходів з протидії тероризму приватні установи і громадські організації

(CERT, ISACA, CSX, CCSIS). Експерти зауважують, що на сьогодні в США у забезпеченні інформаційної безпеки задіяно більш ніж 150 державних організацій і ще більша кількість приватних, які координуються АНБ» [72].

При цьому найважливішою інституцією, що здійснює державне регулювання інформаційної безпеки, є Президент США.

Існуюча організаційно-правова база захисту національного інформаційного простору бере початок з інформаційного забезпечення політики безпеки та функціонування систем оборони та управління в інтересах вищих органів державної влади [34].

Основна правова база інформаційної безпеки в США була сформована після Другої світової війни, коли«американська інформаційна система зіштовхнулася з деструктивним впливом радянської пропаганди. Структурно законодавство США у сфері забезпечення інформаційної безпеки складається як з федеральних законів, так і законів штатів. Незважаючи на існуючи істотні відмінності законів штатів, акти інформаційного законодавства є одними із найбільш уніфікованих, адже в американському суспільстві існує розуміння того, що інформаційна безпека держави є запорукою безпеки кожного громадянина» [34].

Правову основу адміністрування інформаційної безпеки США становлять закони «Про охорону особистих таємниць» (1974 р.), «Про таємницю» (1974 р.), «Про висвітлення діяльності уряду», «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп‘ютерних систем» (1987 р.), «Про комп‘ютерне шахрайство та зловживання» (1986 р.). За ініціативи Президента США Р. Рейгана було розроблено та ухвалено Закон «Про свободу інформації», а забезпечення інформаційної безпеки стало пріоритетним завданням політики Державного департаменту. Пізніше, у 1987 р. прийнято Закон Mb HR-145 «Про забезпечення безпеки ЕОМ», норми якого лягли в основу майбутнього законодавства про кібернетичну безпеку. Цим законом уперше у правовій системі США регламентовано статус нового

інституту – «інформації обмеженого доступу», під якою «американські спеціалісти розуміють несекретну, але важливу з точки зору національної безпеки несекретну інформацію урядових відомств, а також інформаційні дані, що формуються і циркулюють або обробляються в інформаційно-телекомунікаційних системах корпорацій і приватних фірм, що працюють на замовлення уряду США».

Починаючи з 2001 р., коли тодішній президент США Д. Буш під час виступу з промовою перед особовим складом ЦРУ вказав, що «забезпечення інформаційної безпеки є головним пріоритетом у забезпеченні національної безпеки США, у державі починають вводитися у дію загальнофедеральні урядові програми захисту національного інформаційного середовища у комп‘ютерних мережах».

Метою таких програм є «створення всебічно сприятливих умов для розвідувальних органів з метою добування й обробки інформації щодо загроз інформаційному потенціалу інститутів публічного управління з боку інших держав та осіб. Значна увага при цьому приділяється, поряд з негласними інформаційними діями, системному аналізу відкритих джерел і добуванню інформації із конфіденційних баз даних з використанням комп‘ютерного устаткування. Це дало старт формування нормативно-правової бази протидії кіберзлочинності».

Так, у 2003 р. було введено у дію «Національну стратегію безпечного кіберпростору». Пізніше – «Огляд політики кібербезпеки» (2009 р.), «Міжнародну стратегія для кіберпростору» (2011 р.), «Директива Президента США щодо Проекту стратегії покращення кібербезпеки критично важливих об‘єктів інфраструктури» (2013 р.), «Проект стратегії покращення кібербезпеки критично важливих об‘єктів інфраструктури» (2014 р.), Закон про кібербезпеку та обмін інформацією (2015 р.), «Національна стратегія безпеки» (2015 р.), «Стратегія кібербезпеки Департаменту оборони» (2015 р.). Положення цих документів регулюють значний комплекс аспектів забезпечення безпеки електронних інформаційних мереж та ресурсів.

Під час президентства Барака Обами цифрова інфраструктура США була оголошена «стратегічною національною цінністю», а її захист — національним пріоритетом [56].

В основу цієї тези «американський лідер поклав напрацювання наукової доктрини. Мова йде про відому думку американського дослідника аспектів забезпечення інформаційної безпеки Маршалла Макклюєна про те, що в наш час економічні зв‘язки і відносини усе більше набирають форму обміну знаннями, а не обміну товарами» [29, с. 220].

Найважливішим аспектом політики інформаційної безпеки адміністрації Обами є«більш тісне співробітництво держави і бізнесу, що спрямоване, в першу чергу, на захист державних інформаційних ресурсів, а також всього американського інформаційного простору. Для цього необхідно втручання американської держави в інформаційну сферу, в тому числі в інформаційний сектор економіки».

Відповідно, боротьба за гуманітарні ресурси, капітал і ринки стає другосортною «головним зараз стає доступ до інформаційних ресурсів, знань, що призводить до того, що війни ведуться вже більше в інформаційному просторі та за допомогою інформаційних видів озброєнь. Президентом США було сформульовано перелік першочергових безпекових проблем в інформаційній сфері держави: необхідність постійного удосконалення і доопрацювання стратегії забезпечення безпеки інформаційних і комунікаційних мереж, розробка систем попередження та реагування на кібератаки, посилення партнерства держави і приватного сектору у питаннях забезпечення інформаційної безпеки, залучення інвестицій в інноваційні технології, роз‘яснення широким верствам населення переваг необхідності протидії кіберзагрозам» [29, с. 220].

У 2010 р. Президент США підписав «Ініціативу зі всеосяжної національної кібербезпеки», яка органічно доповнила Військову доктрини США. Було покладено початок заснуванню універсальної федеральної мережі захищених каналів зв‘язку, яка б «об‘єднувала усі центри

оперативного реагування на кіберзагрози і хакерські атаки. Було також засновано спеціальні підрозділи кіберконтррозвідки в центральних державних установах США з метою виявлення посягань на державні інформаційні мережі і попередження терористичних атак. Також було розроблено систему управління ризиками для прогнозування ймовірних наслідків несанкціонованого втручання в інформаційні мережі державних установ» [25, с. 152].

Запроваджено роботу програми спеціальної програмної платформи «Ейнштейн», яка «призначена для виявлення втручань у державні інформаційні мережі. З квітня 2012 р. хакерська атака у США кваліфікується як збройна агресія і передбачає весь арсенал заходів реагування. Вражає той факт, що на сьогодні у США 25% коштів, що надходять на науково-дослідні і дослідно-конструкторські роботи, використовуються на розробку систем захисту інформації. Це дуже значні кошти і не кожна держава сучасного світу може це собі дозволити».

Фактично ці документи можна вважати офіційною національною політикою США у сфері інформаційної безпеки, на основі якої формується система державної влади у цій сфері та структура державних органів, що забезпечують інформаційну безпеку в державі.

Визначено пріоритети національної інформаційної політики США: «підтримку досліджень і розробок у галузі інформації і комунікації»; «вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці»; «сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках»; «побудову та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудову глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети»; «збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформація як суспільне благо, інформація як товар, інформація як невіддільний компонент

існування держави (необхідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин)» [37].

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

Рисунок 2.2. Основні державні пріоритети стратегії інформаційної безпеки у США

Примітка: побудоване автором на основі джерела [71].

В рамках розпорядження президента від 11 травня 2017 року №13800 «Посилення кібербезпеки федеральних мереж і критичної інфраструктури» було розроблено нову Національну кіберстратегію (NCS), яка була опублікована у вересні 2018 року [71]. Даний документ «містить цілі, подібні до тих, що поставлені у попередніх схожих документах: політикою у сфері кіберпростору адміністрації Б. Обами 2009» [70] та «Національною стратегію безпеки Дж. Буша» 2002 щодо «безпеки кіберпростору» [73].

Однак, незважаючи на схожість з планами попередніх адміністрацій, NCS Д. Трампа знову викликала «критичні відгуки зі сторони його опонентів, оскільки замість того, щоб продовжувати концепцію зміцнення захисних технологій і мінімізувати вплив інформаційних загроз, адміністрація президента планує посилити наступальні попереджувальні кібероперації та змусити інші країни боятися притягнення до відповідальності за свої дії у відповідь на такі кібератаки зі сторони США. Також критики звернули увагу

на той факт, що дана стратегія жодним чином не вказує на можливості щодо захисту виборів від інформаційних загроз, що є надзвичайно актуальним в світлі подій 2016 р» [75].

В американській політиці апогеєм порушення проблеми інформаційної безпеки США і символічною відправною точкою в її сучасному описі є «російське втручання у американські президентські вибори 2016-го року. Це безпрецедентне явище, оскільки така масштабна кампанія з боку Росії, що була з успіхом проведена, мала місце вперше в контексті історії інформаційної безпеки США. Це був вагомий удар не тільки для інформаційної сфери та національної безпеки країни, але й для американської ідеології та іміджу».

Представники американської влади та спецслужб неодноразово заявляли, що авторитарна Росія намагалася вплинути та вплинула на вибори президента США. Так, у червні 2016 р «американських мас-медіа з'явилася інформація про несанкціоноване втручання в інформаційну систему Національного комітету Демократичної Партії США, особливо було згадано російське «Агенствоінтернет-досліджень» (IRA), яке фінансувалося Євгеном Пригожиним» [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 вона вважала виправданою роками подібних провокацій з боку Сполучених Штатів. Відомо, що кандидатури Г. Клінтон і Д. Трампа до останнього йшли у виборних перегонах з невеликим відривом, і демократи припускають, що якщо б не багаторазове «порушення» кампанії Клінтон електронними листами, викраденими російськими хакерами і опублікованими на WikiLeaks та анти-Клінтонівські повідомлення, об'єктивно спрямовані на підтримку Трампа і розповсюджувані за допомогою соціальних мереж російськими IT-фахівцями, то ситуація могла би змінитись. Однак, президент Трамп та його адміністрація категорично не погоджуються із цією думкою» [64].

У 2017 році було «розпочато розслідування фактів російського втручання у вибори, яке очолив спеціальний прокурор Роберт Мюллер. Розслідування було ініційовано на основі заяв про те, що в період президентської кампанії та перехідного періоду між російськими оперативниками та командою Трампа існувала змова. До розслідування були залучені такі структури, як ФБР, Комітет Сенату з питань розвідки, Постійний окремий комітет з питань розвідки, Судовий підкомітет Сенату з питань злочинності та тероризму, Комітет Палати з питань нагляду та реформування уряду, Судовий комітет Сенату. За результатами розслідування було виявлено, що російське втручання у вибори здійснювалося за трьома напрямками: викрадення та оприлюднення документів основних опонентів Д. Трампа; масове шахрайство на Facebook і Twitter з акаунтами з метою анти-пропаганди Г. Клінтон; спроби співпраці з кампанією Д. Трампа» [43].

Варто підкреслити, що остання теза не знайшла підтвердження, згідно з «Доповіддю Мюллера», який «провів майже два роки на чолі комісії фахівців, розслідуючи зусилля Москви саботувати президентські вибори у США, й оприлюднив свій звіт щодо даної справи, де заявив», що не виявив змови, «незважаючи на численні пропозиції від російських осіб, які допомагали кампанії Трампа» [59].

Загалом серед основних проблем, які стоять перед США у сфері інформаційної безпеки, можна виділити наступні: «зростання встановлення зловмисних програм (вірусів) на мобільні пристрої, поширення вірусів шляхом розповсюдження у магазинах неліцензійного програмного забезпечення, викрадення акаунтів та особистих даних. Так, встановлення вірусних програм на мобільні пристрої протягом 2018 року збільшилося на 45%. Дослідження проведене компанією Symantec показало, що у магазинах, які розповсюджують програмне забезпечення сторонніх розробників, виявлено 99,9% зловмисних програм, що можуть отримувати доступ до персональних даних. Саме на протязі 2018 року у США було викрадено

близько 12 млрд. акаунтів, що містили особисту інформацію, включаючи адресу, номер телефону, номер страхування чи інформацію про кредитну картку. Більш того, у тому ж 2018 році, 45 млн. американців постраждали від викрадення особистих даних, ця цифра значно збільшилася у порівнянні з 2017 роком, в якому 17 млн. споживачів постраждали від викрадення особистої інформації з метою її подальшого використання задля збагачення крадіїв» [66].

Отже, виходячи з наведеного вище матеріалу, ми бачимо чітко визначені проблеми та виклики, з якими Сполученим Штатам постійно доводиться стикатися, як всередині держави, так і за її межами. Останні в комплексі мають значне дестабілізуюче значення для критичної інформаційної інфраструктури, а отже становлять серйозну загрозу національній безпеці держави, окремої особи та суспільства в цілому. Таку ситуацію можна назвати рефлексією на неефективну політику, яку проводить уряд у контексті захисту даних та інформаційної безпеки від посягань, а також наявність постійних міжпартійних суперечок, у тому числі в Конгресі та ЗМІ, які перешкоджають деяким конструктивним прогрес у вирішенні цієї проблеми. 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.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Адаптація зарубіжного досвіду 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, що характеризується розширенням стратегічного мислення, крім оборони, був зумовлений глобалізацією, яка глибоко трансформує саму основу міжнародної системи, стаючи більш нестабільною і непередбачуваною, ніж в часи холодів. Війна, і створює нові загрози. різного характеру. З 2009 року це поняття включено до французького оборонного кодексу.

Іншою особливістю Білої книги з питань оборони та національної безпеки 2008 року є те, що вона визначає загрози для використання інформаційних систем і засобів масової інформації. Таким чином, характеризуючи загрозу широкомасштабних атак на інформаційні системи, зазначається, що останні пронизують основні системоутворюючі ланки економічного та соціального життя.

Таким чином, «залежність від інформаційних систем інженерних комунікацій, транспортної інфраструктури, продовольчого забезпечення і навіть управління обороною, робить сучасне суспільство та його безпеку вразливими до випадкових пошкоджень та цілеспрямованих атак, які здійснюються через обчислювальні мережі. Загроза шпіонажу та стратегічного впливу обґрунтовується поширенням застосування у міждержавних відносинах засобів «м'якої сили», маніпулюванням свідомістю через ЗМІ та Інтернет, посяганнями на науковий, економічний, оборонний потенціал Франції та її території, небезпекою культурної експансії» [10, с. 456].

Четверта Біла книга була опублікована в 2013 році під головуванням Франсуа Олланда. П'ятий документ має дещо іншу назву «Стратегічний оборонний огляд та національна безпека» опубліковано в кінці 2017 року під головуванням Еммануїла Макрона.

В Оборонному огляді значна увага приділяється «інформаційним загрозам та заходам протидії ним. Так, зазначається, що у кіберпросторі деякі напади через їх масштаби і серйозність можуть бути віднесені до категорії

збройної агресії. Труднощі з розподілом акцій і поєднання прямих дій з методами впливу і пропаганди уможливлюють безліч сценаріїв інструменталізації з метою дестабілізації або підтримки простіших операцій».

Облік кіберзагроз та їх еволюції тим складніший, що «він не може обмежуватися периметром оборони через заплутування питань і участі державних і приватних суб'єктів. У зв'язку з цим наголошується, що армії повинні повністю планувати і проводити операції в цифровому просторі аж до тактичного рівня в ланцюжку планування і проведення кінетичних операцій. Операції в цифровому просторі розширюють діапазон традиційних ефектів, доступних політичній владі, і використовують зростаюче оцифрування опонентів Франції, як державних, так і недержавних. Ця здатність вимагає посилених і досить гнучких людських ресурсів, а також постійної розробки конкретних технічних рішень» [62].

Крім того, для забезпечення інформаційної безпеки в DefenseReview дозволяється ведення бойових дій у кіберпросторі, що означає оборонну або наступальну боротьбу в усьому цифровому середовищі проти урядових чи неурядових опонентів.

Стратегії національної безпеки, викладені в Білих книгах, є основою законів про військове планування. Сьогодні чинний французький закон «Про військове планування на період з 2019 по 2025 рік та інші положення, що стосуються оборони» № 2018-607 від 13.07.2018. Для Франції серйозною загрозою її інформаційному простору залишається так званий «кіберджихадизм», який «полягає у застосуванні Інтернет-технологій та послуг, особливо соціальних мереж, в просуванні джихадизм насильства. Він здійснюється шляхом злому урядових сайтів, корпоративних сайтів або організацій, пропаганди і вербування. Заходами протидії йому виступають: блокування сайтів та акаунтів, створення контрпропагандистських сайтів тощо».

Система інформаційної безпеки Франції складається з таких спеціальних структур: «Національне агентство безпеки інформаційних систем (ANSSI), Служба аудіовізуальних матеріалів (Serviceaudiovisuel), Міжвідомчий директорат з питань інформаційних систем та зв'язку (DISIC), Директорат з розвитку засобів масової інформації (DDM) та деякі інші».

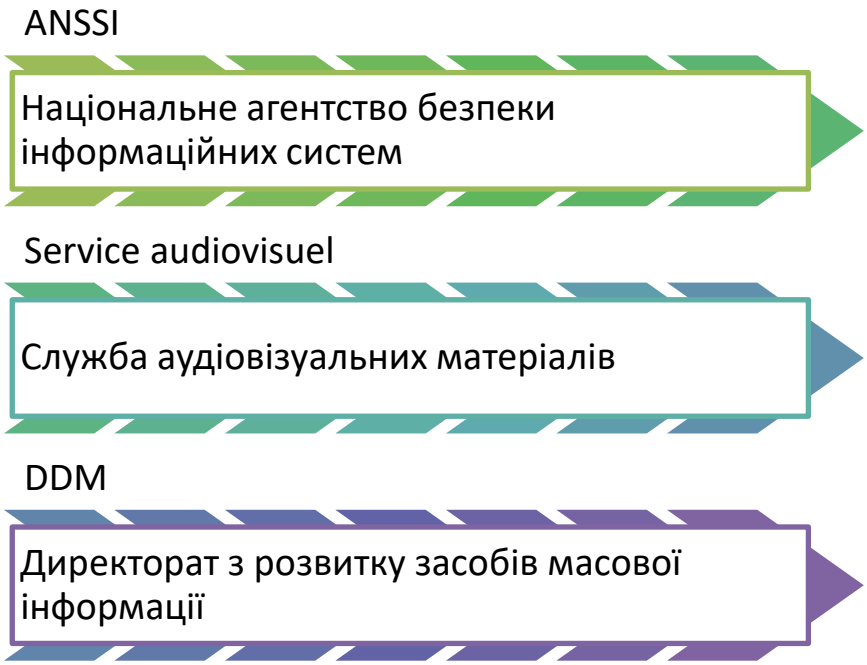

Рисунок 3.1 Система інформаційної безпеки Франції

Примітка: побудоване автором на основі джерела [51]

Національне агенство безпеки інформаційних систем (ANSSI) – «французька служба з національною компетенцією, створена декретом в липні 2009 року, підпорядковується Генеральному секретаріату оборони та національної безпеки».

ANSSI відповідає за просування технологій, «систем і національного досвіду з метою сприяння впровадженню цифрової економіки. Водночас основні зусилля фахівців ANSSI спрямовані на реалізацію заходів, викладених у національній стратегії безпеки та оборони. Основними цілями агентства є: підвищення ефективності управління та координації діяльності органів державної влади, суб'єктів критичної інфраструктури, суспільства в умовах інформатизації; забезпечення промислової безпеки; організація

захисту національної інформаційно-телекомунікаційної інфраструктури в умовах військової загрози, в тому числі кібервійни; підтримка технічних засобів, необхідних для виконання покладених на агентство завдань, в актуальному стані. До його повноважень належать» [51]:

– «формування державної політики у сфері оборони та безпеки інформаційних систем»;

– «розробка організаційно-правових та технічних заходів захисту державних інформаційних систем та контроль за їх виконанням»;

– «моніторинг, виявлення, оповіщення і реагування на кібератаки, спрямовані на державні інформаційно-телекомунікаційні системи»;

– виявлення і реагування на вірусні атаки, реалізація адаптаційних механізмів захисту від них;

– «запобігання загрозам через сприяння розробці програмного забезпечення та засобів обчислювальної техніки, яким можна довіряти»;

– «консультативна функція і підтримка суб'єктів критичної інфраструктури»;

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

– «розробка і придбання основних продуктів, призначених для захисту найбільш чутливих ділянок міжвідомчої державної мережі»;

– «реалізація засобів контролю управління і зв'язку з питань оборони і національної безпеки»;

– «сертифікація комплексних систем захисту інформації» [51].

У реалізації інформаційної політики у Франції «бере участь і Служба аудіовізуальних матеріалів (Serviceaudiovisuel), яка діє при канцелярії Президента. Служба проектує аудіовізуальні технічні платформи Президента Республіки, організовує його виступи та забезпечує їх трансляцію по всій території країни і за кордоном».

Крім того, Служба веде фотовідділ про діяльність Президента та життя Єлисейського палацу, керує банком фотографій та взаємодіє із ЗМІ та

громадськістю. Важливою функцією цієї Служби є аудіовізуальний моніторинг ЗМІ та формування відповідного архіву матеріалів. Загалом його діяльність спрямована на формування іміджу Президента.

Враховуючи активну інформатизацію діяльності органів державної влади у складі Генерального секретаріату Уряду (SGG), що «підпорядковується Прем'єр-міністру, на початку 2011 року (Декрет № 2022-193 від 21.02.2011) було створено Міжвідомчий директорат з питань інформаційних систем та зв'язку (DISIC). Він відповідає за функціонування інформаційно-телекомунікаційних систем, призначених для обміну інформацією між різними відомствами та з громадянами. Основними завданнями підрозділу є: проектування інформаційно-телекомунікаційної інфраструктури уряду з урахуванням потреб діяльності та оптимізації ресурсів, організація закупівлі обладнання, програмного забезпечення та інформаційних послуг, розподіл електронно-обчислювальної техніки між міністерствами, впровадження нових інформаційних систем, забезпечення стратегічного планування розвитку інформаційної інфраструктури».

Метою створення DISIC є «моніторинг тенденцій у галузі інформаційних технологій, оптимальне використання інформаційних ресурсів завдяки спільним банкам даних, запобігання ризикам безпеки інформації, пов'язаним із впровадженням масштабних проектів, підвищення обслуговування користувачів інформаційних систем» [10, с. 301].

Основним законом у сфері інформаційної безпеки в Німеччині є Закон «Про посилення безпеки систем інформаційних технологій» (Закон про безпеку IT) від 25.07.2015. Закон відводить Федеральному відомству з безпеки в сфері інформаційних технологій (BSI) центральну роль в захисті критично важливих інфраструктур у Німеччині.

При цьому під критичними інфраструктурами розуміються об'єкти, установки або їх частини, які «належать до секторів енергетики, інформаційних технологій і телекомунікацій, транспорту і дорожнього руху, охорони здоров'я, водопостачання, харчування, фінансів і страхування. Такі

об’єкти мають велике значення для функціонування спільноти, тому що їх зупинка або погіршення роботи призведе до значного дефіциту поставок або створить загрози громадській безпеці. 27 березня 2019 Федеральне міністерство внутрішніх справ також опублікувало проект закону про безпеку інформаційних технологій, в якому міститься цілісний підхід до безпеки вказаної сфери».

Крім іншого, «передбачається запровадження зручного для споживача ярлика IT-безпеки для комерційних продуктів, а також посилення компетенції BSI і розширення переліку правопорушень у сфері кібербезпеки і пов’язаних з ними слідчих дій. Законопроект також збільшує кількість адресатів звітності та зобов’язань. Загалом закон, як очікується, створить певні економічні складнощі для компаній і органів державної влади» [57].

Забезпечення інформаційної безпеки Німеччини здійснюють Федеральні збройні сили Німеччини (Бундесвер), зокрема, «відділом інформаційних та комп’ютерних мережевих операцій командування стратегічної розвідки. Командування стратегічної розвідки також здійснює управління супутниковою розвідувальною системою SAR-Lupe, яка була запущена в грудні 2008 р».

За допомогою п’яти супутників система SAR-Lupe, яка «вважається однією з найдосконаліших систем у своєму роді, може передавати зображення з роздільною здатністю менше одного метра не залежно від денного світла і погоди. Таким чином, можна пояснити майже будь-яку точку на землі. Система збирає й оцінює інформацію про військово-політичну ситуацію в окремих країнах і альянсах потенційного або фактичного противника і його збройних сил».

Отже, проаналізувавши досвід країн ЄС із системи забезпечення інформаційної безпеки, варто зауважити, щосьогодні не існує універсального підходу чи єдиної моделі управління інформаційною безпекою. Кожен регіон світу і країни має 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 збільшення бюджету, збільшення штату, технологічне лідерство та міжнародне співробітництво.

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 у Законі України «Про основи національної безпеки» однією з основних загроз інформаційній безпеці є «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [3].

Доктрина інформаційної безпеки України визначає такі загрози

інформаційній безпеці країни: «поширення у світовому інформаційному просторі спотвореної, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України»; «зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також Інтернет»; «деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України»; «прояви сепаратизму в ЗМІ, а також в Інтернеті за етнічною, мовною, релігійною та іншими ознаками» [32].

Як зазначає Р. Р. Марутян, «найсуттєвішою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя. Метою таких інформаційних операцій є забезпечення власних національних інтересів інших держав» [19, с. 89].

До загроз інформаційній безпеці України в інформаційній сфері також варто зарахувати: «прояви обмеження свободи слова та доступу громадян до інформації»; «викривлення, спотворення, блокування, замовчування упереджене та тенденційне висвітлення інформації»; «несанкціоноване її поширення; відкриту дезінформацію»; «інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через ЗМІ на населення і громадськість менш потужної держави»; «виникнення і функціонування у національному інформаційному просторі держави непідконтрольних й інформаційних потоків тощо».

Проти України широко застосовуються сучасні технології негативного інформаційно-психологічного впливу, які стають загрозою для українського національного інформаційного простору та державного суверенітету. Гарантування інформаційної безпеки України в умовах дестабілізуючих негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської Федерації потребує консолідації зусиль на всіх рівнях державної влади та громадянського суспільства.

В якості протидії широкомасштабним негативним інформаційно-психологічним впливам, операціям і війнам слід визначити пріоритетні напрямки державної інформаційної політики та важливі кроки з боку української влади [8, с. 106]:

1) «інтеграція України до світового та регіонального європейського інформаційного просторів»;

2) «інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації»;

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

4) «модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики»;

5) «удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів»;

6) «розвиток національної інформаційної інфраструктури»;

7) «підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг тощо» [8, с. 107].

З метою недопущення інформаційного розширення діяльність держави в інформаційному просторі має здійснюватися за такими напрямами:

1) «реалізація упереджувальної стратегії та тактики (превентивні заходи)»;

2) «здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ)»;

3) «захист національного інформаційного простору. Головна ціль – забезпечення домінування та медійної переваги в інформаційному просторі».

Варто зазначити, що «з метою захисту національного інформаційного простору, створення ефективної системи забезпечення інформаційної безпеки, з боку української влади здійснюються певні заходи. Зокрема, 14 січня 2015 року Кабінет Міністрів України ухвалив Постанову, згідно з якою створено Міністерство інформаційної політики України, пріоритетними завданнями якого є протидія інформаційній агресії з боку Російської федерації; розроблення ефективної стратегії інформаційної політики держави та Концепції інформаційної безпеки України; узгодженість та координація функціонування і діяльності органів державної влади і інформаційній сфері».

З метою протидії негативним наслідкам інформаційної пропаганди та інформаційних воєн, нейтралізації та запобігання реальним і потенційним загрозам в інформаційному просторі України РНБО України ухвалила рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України».

У документі йдеться, що РНБО, враховуючи необхідність удосконалення нормативно-правового забезпечення та запобігання та нейтралізації потенційних та реальних загроз національній безпеці в інформаційній сфері, ухвалила рішення: «розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів»; «посилити контроль за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки»; «ужити заходів щодо забезпечення поширення у світі об’єктивних відомостей про суспільно-політичну ситуацію в Україні» [2].

Необхідність створення національної системи інформаційної безпеки очевидна, «колинею будуть займатися відповідні підрозділи СБУ, кіберзахистом – відповідні підрозділи ДССЗЗІ (Державної служби спеціального зв'язку та захисту інформації), а боротьбою з кіберзлочинністю – відповідні підрозділи МВС. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО» [30].

Національна система інформаційної безпеки створюється і розвивається «відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини у сфері національної безпеки, зокрема: Закон України «Про основи національної безпеки України», Концепція розвитку сектору безпеки і оборони України, Положення про Національний координаційний центр кібербезпеки, Стратегія національної безпеки України, Стратегія кібербезпеки України, Воєнна доктрина України, Доктрина інформаційної безпеки України тощо.

Війна в кіберпросторі спричиняє нові кіберзагрози. Кіберзагрози – це «наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем» [13, с. 88].

Створення національної системи інформаційної безпеки передбачено Стратегією кібербезпеки для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави.

Організаційне забезпечення системи інформаційної безпеки також можна розглядати як цілеспрямовану діяльність суб'єкта інформаційної безпеки, пов'язану з:

– «створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі»;

– «впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень».

Національна система інформаційної безпеки має, насамперед, «забезпечити взаємодію з питань інформаційної безпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури. Основу національної системи інформаційної безпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи» [36].

Аналізуючи системи інформаційної безпеки провідних країн світу, робимо висновок, що на сьогодні не існує єдиної моделі побудови національної системи інформаційної безпеки.

Стратегія інформаційної безпеки Канади «визначає кібертероризм та ворожі дії в кіберпросторі з боку інших країн (кібершпигунство і кібервійну) основними загрозами кібернетичній безпеці держави, а ключовим органом, на який покладена координація та контроль за імплементацією вказаної Стратегії, реалізація державної політики та координація заходів у сфері кібербезпеки та протидії кіберзагрозам, визначене Міністерство громадської безпеки Канади».

Стратегія кібербезпеки Австрії «національним координатором і центральним органом у сфері інформаційної безпеки визначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ Австрії. Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері інформаційної безпеки та боротьби з кіберзлочинністю».

Агентство внутрішньої безпеки відіграє ключову роль у забезпеченні інформаційної безпеки Польщі (АВБ) – «польський контррозвідувальний

орган. Так, у 2013 р. АВБ розробило Стратегію інформаційної безпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони Польщі, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій (активний кіберзахист)» [36].

Аналіз нормативно-правових та організаційних основ системи інформаційної безпеки провідних країн світу свідчить«про домінантну роль спецслужб у забезпеченні кібернетичної безпеки держави, що пов'язано із характером кібернетичних загроз сьогодення, протидія яким потребує інструментарію (повноважень, форм і методів), притаманного виключно спеціальним, а саме, контррозвідувальним органам держави».

Враховуючи міжнародний досвід та з метою ефективного вирішення проблем кібербезпеки держави, відомство, яке «здійснює координацію діяльності всіх суб'єктів забезпечення кібернетичної безпеки (Національної системи інформаційної безпеки), доцільно визначити Службу безпеки України, яка є спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності, а також протидіє внутрішнім та зовнішнім загрозам, у тому числі в інформаційній (кібернетичній) сфері.

Також, зважаючи на світову практику, було запропоновано створити Національний центр кібербезпеки, який повинен був підпорядковуватися СБ України» [12, с. 77].

Особливу увагу приділяю національній системі інформаційної безпеки України «на Команді реагування на комп'ютерні надзвичайні події України – спеціалізованому структурному підрозділі Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України, який заснований у 2007 р. Метою діяльності CERT-UA є забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. Діяльність CERT-

UA передбачена» Законом України «Про Державну службу спеціального зв'язку та захисту інформації», Законом України «Про телекомунікації» та підзаконними актами.

Україні необхідно «створити ключові механізми державного управління інформаційною безпекою в умовах кіберзагроз у вигляді спеціалізованих центрів, інститутів та експериментувати з операціями щодо ведення інформаційної війни, фінансувати експертні дослідження у сфері інформаційних операцій і створювати структури для наукових досліджень і та дослідно-конструкторських розробок».

На порядку денному стоїть завдання «поетапно сформувати індустрію програмного забезпечення»; «пришвидшити роботи щодо створення української національної мережі суперкомп'ютерних комплексів, об'єднаних високошвидкісними оптико-волоконними каналами передачі даних»; «сформувати чітку інформаційну політику з просування вітчизняних IT-компаній за кордоном; об'єднати інтереси освіти, науки та IT-бізнесу»; «визначити базові вищі навчальні заклади, на основі яких сформувати кластери, що дадуть змогу вирішувати питання кадрової підготовки фахівців IT-технологій» [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. Вважаємо, що запропоновані принципи допоможуть уникнути фрагментації у формуванні національної системи інформаційної безпеки. Визначені 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 безпекив 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 державної таємниці. 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, їх інформаційних систем від кібернетичних атак; вдосконалення засобів виявлення кібератак 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.

В США існують чітко визначені проблеми та виклики у забезпеченні інформаційної безпеки, з якими доводиться постійно стикатися, як всередині держави, так і за її межами. Основним завданням органів публічної влади в таких умовах - 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 впливає 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. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» затвердженоУказом Президента Українивід 25 лютого 2017 року № 47/2017. URL:https://zakon.rada.gov.ua/laws/show/47/2017#Text.
2. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. URL: http://www.zakon5.rada.gov.ua /laws/ show/n0004525-14.
3. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
4. Про створення у структурі ДСБЕЗ підрозділів по боротьбі з правопорушенням у сфері інтелектуальної власності та високих технологій: Наказ МВС України від 31.05.2001 р., № 429.
5. Баранов А.А., Брижко В.М., Базанов Ю.К. Права людини і захист персональних даних. 2017. 509с.URL: library.khpg.org/files/docs/Kn_L_.pdf.
6. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми. 2018 рік.URL: Режим доступу: http://www.crime-research.iatp.org.ua/library/strateg.htm
7. Бухарин В. В. Сравнительныйанализнормативнойбазы по обеспечениюинформационнойбезопасности в США и РоссийскойФедерации (конец XX – начало XXI В.). ВестникИрГТУ. 2016. № 12. С. 101 – 108
8. Даник Ю., та Корнейко О. Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України, 2018. С. 105-123.

9. Жигалкин Ю. ДоказательствавмешательстваРоссии в выборы президента США. 2019. 434 с. URL: https://www.svoboda.org/a/usa-russia-indictment/29044968.html
10. Забезпечення інформаційної безпеки держави : підручник. Київ : ДНУ «Книжкова палата України», 2018. 672 с.
11. Кельман М. О. Загальна теорія держави і права: підруч. Київ: Кондор, 2006. 477 с.
12. Климчук О.О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3. С. 75–83.
13. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України. Демократичне врядування. 2014. Вип. 14 URL: http://nbuv. gov.ua/UJRN/DeVr_2014_14_5.
14. Колпаков В. К. Адміністративне право України: підруч. Київ: Юрінком Інтер, 2009. 736 с.
15. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) автореф. дис ... канд. політ. наук: 21.01.01 / Вікторія Констянтинівна Конах. Нац. ін-т стратег. дослідж. Київ, 2005. 20 с.
16. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. Київ: Кондор, 2018. 382 с.
17. Логунов А. Б. Региональная и национальнаябезопасность: учеб. Пос. Москва: Вузовскийучебник, 2009. 432 с.
18. Маклаков Г. Ю. Анализсплоченностистуденческойгруппы в работе куратора. Структурно-системныйподход в обучении и воспитании. – Днепропетровск : ДГУ, 1984. С. 129131.
19. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України 2018. URL: http://www.dsaua.org/index.

php?option=com_content&view=article&id=198%3A2014-08- 13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid= 90&lang=uk.

20. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи 2016. URL: http://www.justinian.com.ua/article.php?id=3222
21. Почепцов Г. Г. Інформаційна політика: навч. посіб. Київ : Знання, 2006. С. 130–211.
22. Рекомендация МСЭ-Т Х.1205. Обзоркибербезопасности. Женева : МСЭ, 2009. С. 55.
23. Советский энциклопедический словарь ; гл. ред. Прохоров А.М. [4-е изд.].М. : Сов. энциклопедия, 1986. 1600 с.
24. Стрельцов А. А. ОбеспечениеинформационнойбезопасностиРоссии. Теоретические и методологическиеосновы / А. А. Стрельцов; под ред.: В. А. Садовничего и В. П. Шерстюка. М.: МЦНМО, 2002. С. 153-168.
25. Телеховський Ю. Досвід трансформації спецслужб Угорщини: висновки для Україїни. Стратегічні пріоритети. № 3(28). 2019 р. - С. 151-155.
26. Туманова Л. В. Обеспечение и защита права на информацию. Москва: Городец-издат, 2001. 345 с.
27. Уфимцев Ю. С. Методика информационной безопасности. Москва: Экзамен, 2004. 544 с.
28. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320.
29. Щепанківський В. Г. Інформаційна безпека як складова образу країни. Актуальні проблеми міжнародних відносин. 2011. Вип. 102. Ч. 1. С. 219– 228.
30. В Україні буде створена Національна система кібербезпеки, 27 січня 2016 URL: http://zaxid.net/news/showNews.do?v_ukrayini_bude_ stvorena_natsionalna_sistema_ kiberbezpeki&objectId=1380648.

31. Вопросы информационной безопасности и СНГ. URL: http://lawbook. online/pravovoe-regulirovanie-mejdunarodnoe/voprosyi-informatsionnoy-bezopasnosti-15115.html.
32. Доктрина інформаційної безпеки України URL: http://www.zakon3.rada.gov.ua/laws/ show/514/2009.
33. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. – Holland, DenHaag: NationalCoordinatorforSecurityandCounterterrorism, 2013. – URL: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2 Engelseversie.
34. Політика гарантування інформаційної безпеки в Україні. Інтернет-сайт «Проблеми інформаціної безпеки України». URL: https://sites.google.com/site/bezpekiukraien223/politika-garantuvanna-informacijnoie-bezpeki-v-ukraieni.
35. Польща створює Доктрину інформаційної безпеки URL:http://www.eurointegration.com.ua/news/2015/07/26/7036321/.
36. Стратегія кібербезпеки України від 14.05.2021 року. URL: http://zakon3. https://www.president.gov.ua/documents/4472021-40013.
37. Укрінформ. Трамп ігнорує серйозні загрози для національної безпеки з боку Росії. URL : https://www.ukrinform.ua/rubric-world/2184991-so-i-ak-skazav-tramp-kongresu.html.
38. По всій Європі? Кіберзахист нації: URL: http:// archive.defensenews.com/ article/20130709/DEFREG01/307090008/Across-Europr-Nations-Mold-Cyber-Defenses.
39. Закон про електронну інформаційну безпеку центральних і місцевих органів влади. URL:http://njt.hu/cgi_bin/njt_doc.cgi?docid= 160206.240508.
40. Закон про Федеральне управління інформаційної безпеки (BSI Act - BSIG): URL:https://www.bsi.bund. de/DE/DasBSI/Gesetz/ gesetz.html.
41. Побудова інформаційного суспільства: переміщення Канади в 21 століття.

[НормативнийдокументМіністерстваПостачаннятаПослугКанади] / Міністерство постачання та послуг. — Оттава, 1996.

42. Стратегія кібербезпеки Канади: для сильнішої та процвітаючої Канади. Її Величність Королева в правовій частині Канади, 2010. 14 с.
43. CNN. Короткі факти розслідування президентських виборів 2016 року. URL: https://edition.cnn.com/2017/10/12/ us/2016-presidential-election-investigation-fast-facts/index.html
44. Повідомлення Комісії із захисту критичної інформації інфраструктури: захист Європи від широкомасштабних кібератак і зброї: підвищення готовності, безпеки та стійкості. COM (2009)149: URL:http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.
45. Повідомлення Комісії: До загальної політики боротьби з кіберзлочинністю. COM (2007): URL:http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf
46. Повідомлення Європейської комісії: Безпека мереж та інформації: пропозиція щодо європейського політичного підходу. COM (2001) 298: URL:http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf.
47. Протидія кібертироризму. URL:http://msz.gov.pl/en/foreign_policy/security_policy/intemational_terrorism/countering_cyber_terrorism/&printMode=true
48. Стратегія кібербезпеки для Німеччини. Берлін: Федеральне міністерство внутрішніх справ. – 2011. 15 с.
49. Стратегія кібербезпеки. Співдружність Австралії: уряд Австралії, 2009.URL:www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber %20Security%20Strategy%20-%20for%20website.pd
50. Кібер та інформаційний простір. URL: bundeswehr.de/portal/a/cir/start.

51. Указ №2009-834 від 07 липня 2009 року про створення служби національної компетенції під назвою «Національне агентство безпеки інформаційних систем.
URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= JORFTEXT000020828212&dateTexte= &categorieLien=id.
52. Резолюція Генеральної Асамблеї «Право на приватність у цифрову епоху», A/RES/68/167: URL: Mhttp://www. ohchr.org/EN/Issues/ DigitalAge/Pages/DigitalAgelndex.aspx.
53. Закон про вимоги та процедури федеральних перевірок безпеки та захисту секретної інформації. Закон про перевірку безпеки- SÜG: URL:http://www. gesetze-im-intemet.de/s_g/ BJNR086700994.html.
54. Стратегія національної безпеки Угорщини (2012): URL:http://2010-2014.kormany.hu/download/4/32/ b0000/National%20Security% 20Strategy.pdf
55. Закон Республіки Хорватії про інформаційну безпеку (2007): URL:http://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/ Information-Security-Act.pdf
56. Міжнародна стратегія кіберпростору. Білий дім. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
57. 57-й Закон про IT-безпеку (IT-SiG) 2.0. Коротко про найважливіші зміни до законопроекту. Спільнота Бека. Отримано 3 квітня 2019 року. URL: https://community.beck.de/2019/04/03/it-sicherheitsgesetz-it-sig-20-die-wichtigsten-aenderungen-desreferentenentwurfs-im-schnellueberblick.
58. Лора Чаппелл, Пелгрейв Макміллан. Німеччина, Польща та спільна політика безпеки та оборони: зближення перспектив безпеки та оборони в розширеному ЄС. 29 серпня 2012. 232 с.
59. Маццетті М., Беннет К., Мюллер. Резюме доповіді. URL: https://www.nytimes.com/2019/03/24/us/ politics/mueller-report-

summary.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking

60. Національна стратегія кібербезпеки та План дій на 2013-2014 роки. Турецька республіка. Міністерство транспорту, морських справ та зв'язку, 2013. С. 47.
61. NemzetiAdatvedelmiesInformacioszabadsagHatosag (Національних орган Угорщини із захисту даних та свободи інформації): URL: http://www.naih.hu/uegyfelszolgalat, kapcsolat.html.
62. Стратегічний огляд: чіткий і добровільний аналіз для підготовки до наступного закону про військову програмування. 2017. URL: https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.
63. Сайфер Інтернет Програми: URL: http: //ec.europa.eu/ information_society/activities/sip/policy/ programme/current_prog/index_en.htm.
64. Шейн С., Маццетті М. Сюжет підриву виборів: розгадка історії Росії досі. 2021 рік.
URL: https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html
65. 65-й Закон про документи Штазі (Stasi-Unterlagengesetz, StUG): URL: http://germanlawarchive.iuscomp. org/?p=714.
66. Корпорація Symantec. 10 фактів і статистики кібербезпеки за 2018 рік. URL: https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-youshould-know.html
67. Використання можливостей - уникнення ризиків. URL: https://www.bsi/bund.de//EN/Home/ home_node.html$jsessionid=EA326461A185448F29C194C194C91BC85F23.2_cid286.
68. Закон про захист даниї телепослуг. URL:http://ourworld.compuserve.com/homepages/ckuner/multimd.

69. Національна стратегія кібербезпеки республіки.
URL: http://www.uvns.hr/UserDocsImages/ en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.
70. Білий дім. Огляд кібербезпеки. Вашингтон, округ Колумбія, березень 2009р., 47с.
URL : https://obamawhitehouse.archives.gov/cyberreview/documents/.
71. Білий дім. Національна кіберстратегія Сполучених Штатів Америки. Вашингтон, округ Колумбія, вересень 2018р.,29с. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
72. Білий дім. Стратегія національної безпеки Сполучених Штатів Америки. Вашингтон, грудень 2017р., 56с. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
73. Білий дім. Стратегія національної безпеки, Вашингтон, вересень 2002р. URL: https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/.
74. Захист Конституції (Bfv): URL:http://www. verfassungsschutz.de.
75. Безрозсудна стратегія кібербезпеки Вольфа Дж.Трампа. URL: https://www.nytimes.com/2018/10/02/ opinion/trumps-reckless-cybersecurity-strategy.html.

Виконала: слухачка магістратури за спеціальністю «Публічне управління та адміністрування»
«____»_____2021р. _____ **А.Р.Тимощук____**
Підпис _____
Ініціали, прізвище

Науковий керівник:
Кандидатка наук з державного управління, доцента **Т.В. Гаман**
_____ _____
Підпис Ініціали, прізвище

Робота допущена до захисту:

Завідувач кафедри публічного управління та адміністрування, доктор наук з державного управління, доцент **Е.В.Щепанський**
«___»_____2021 р. _____ _____
Підпис Ініціали, прізвище