МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЛІНГВІСТИКИ ТА СОЦІАЛЬНИХ КОМУНІКАЦІЙ
КАФЕДРА ІСТОРІЇ ТА ДОКУМЕНТОЗНАВСТВА

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ (І. І. Тюрменко)
«_____»_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ВИШОЇ ОСВІТИ
ОС «МАГІСТР»

Тема: «Організація захисту інформації в Секретаріаті Кабінету Міністрів України».

Виконавець: здобувач вищої освіти ДК-221 М Слюсар Ігор Володимирович

Керівник: доктор історичних наук, професор Ірина Іванівна Тюрменко

Нормоконтролер: кандидат історичних наук, доцент Халецька Леся Петрівна

_____
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет лінгвістики та соціальних комунікацій
Кафедра історії та документознавства
Галузь знань – 02 «Культура і мистецтво»
Спеціальність – 029 «Інформаційна, бібліотечна та архівна справа»
Освітня програма – «Документознавство та інформаційна діяльність»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ І. І. Тюрменко

«____»_____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Слюсара Ігоря Володимировича

1. Тема кваліфікаційної роботи: «Організація захисту інформації в Секретаріаті Кабінету Міністрів України» затверджена наказом ректора від «19» вересня 2023 р. № 1834/ст.

2. Термін виконання роботи: з 25.09.2023 р. до 31.12.2023 р.

3. Вихідні дані до роботи: робота складається зі вступу, трьох розділів, висновків, списку використаних джерел загальним обсягом 109 сторінок, з них обсяг основного тексту – 93 сторінки, список використаних джерел нараховує 80 позицій, 2 додатки, 6 ілюстрацій.

4. Зміст пояснювальної записки: Розділ 1. Теоретико-методологічні аспекти захисту інформації в Україні; Розділ 2. Організаційні засади захисту інформації в Україні; Розділ 3. Вимоги до забезпечення захисту інформації в СКМУ; Висновки; Список використаних джерел; Додатки.

5. Перелік обов’язкового ілюстративного матеріалу: Керівники Структурних підрозділів Секретаріату КМУ; База даних «Законодавство України»; один з нормативно-правових актів інформаційної безпеки в Секретаріаті Кабінету Міністрів України; скріншот вебсайту «Урядовий портал»; скріншот вебсайту Міністерства цифрової трансформації; скріншот вебсайту Міністерства культури та інформаційної політики України.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Визначення та обґрунтування теми кваліфікаційної роботи	02.09.2023	
2.	Оформлення завдання на виконання кваліфікаційної роботи. Складання плану роботи. Узгодження з керівником	08.09.2023	
3.	Визначення об’єкта, предмета, мети, завдань дослідження. Підбір, опрацювання, вивчення літератури та джерел з теми дослідження	18.09.2023	
4.	Виконання індивідуальних завдань з теми роботи	22.09.2023	
5.	Написання основної частини, вступу та висновків	30.10.2023	
6.	Оформлення роботи та подання її на перше читання керівникові	02.11.2023	
7.	Опрацювання зауважень та виправлення недоліків	10.11.2023	
8.	Попередній захист кваліфікаційної роботи	30.11.2023	
9.	Проходження нормоконтролю	01.12.2023	
10.	Подання роботи на перевірку на плагіат	07.12.2023	
11.	Подання роботи на рецензування	11.12.2023	
12.	Подання остаточного варіанта на кафедру	18.12.2023	
13.	Захист роботи	25.12.2023	

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв

8. Дата видачі завдання: «08» вересня 2023 р.

Керівник кваліфікаційної роботи _____ І.І. Тюрменко
(підпис керівника)

Завдання прийняв до виконання _____ І.В. Слюсар
(підпис випускника)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи ОС «Магістр» на тему: «Організація захисту інформації в Секретаріаті Кабінету Міністрів України»: 109 сторінок, 2 таблиці, 6 ілюстрацій, 80 використаних джерел, 2 додатки.

ІНФОРМАЦІЯ, ЗАХИСТ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, БЕЗПЕКА ІНФОРМАЦІЇ, СЕКРЕТАРІАТ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ.

Об’єкт дослідження – захист інформації в органах виконавчої влади України.

Предмет дослідження – специфіка організації інформаційної безпеки в Секретаріаті КМУ, безпека інформації в кіберпросторі.

Мета дипломної роботи полягає в узагальнені знань щодо інформаційної безпеки в Україні та в Секретаріаті Кабінету Міністрів України.

Методи дослідження. У роботі використані загальнонаукові методи: методи аналізу та синтезу, історичний метод, бібліографічної евристики, спостереження, узагальнення.

У рамках даного дослідження було проведено аналіз наукових статей за темою роботи; розглянуто нормативно-правові акти, які забезпечують організацію захисту інформації. Охарактеризовано важливість ролі та загрози в захисті інформації під час діяльності установ та організацій. В кваліфікаційній роботі розглянуті вимоги до забезпечення захисту інформації в Секретаріаті Кабінету Міністрів України. Було встановлено, що ця державна установа має різні рівні секретності, тому більшість інформації відноситься до державної таємниці, або є конфіденційною. Отже, інформаційна безпека в даній установі є комплексною та застосовується для захисту інформації та паперових носіях, так і електронних. Особливої уваги надається захисту комп’ютерів від несанкціонованого втручання.

Було встановлено, що партнерство у сфері захисту інформації є важливим фактором забезпечення інформаційної безпеки в Україні. Воно передбачає співпрацю між різними суб’єктами інформаційної діяльності, зокрема органами державної влади, органами місцевого самоврядування, профільними установами та організаціями, а також міжнародними організаціями.

ЗМІСТ

ВСТУП

Актуальність теми. На сьогоднішній день актуальність теми організації захисту інформації надзвичайно висока, оскільки умови сучасної інформаційної ери створюють нові виклики та загрози для національної безпеки та стабільності держави. Зокрема, Україна, як країна, яка зазнала кібератак та інформаційної війни, стикається із складним завданням забезпечення безпеки своїх інформаційних ресурсів та інфраструктури перед новими формами загроз.

Зростання кількості кібератак та кіберзлочинів, спрямованих як на державні, так і на громадянські об’єкти, робить захист інформації надзвичайно важливим завданням для держави та її громадян. Інформаційні атаки можуть мати серйозний вплив на функціонування суспільства, економіки та політичної системи. Захист інформації став необхідністю, і розробка та вдосконалення систем захисту інформаційної безпеки стають актуальними завданнями.

Розвиток нових технологій і зміни в соціально-політичній ситуації в Україні створюють потребу в постійному аналізі та вдосконаленні заходів зі збереження та захисту інформації в умовах загрози. Важливим є також розгляд перспектив розвитку системи захисту інформації та підготовка до нових викликів у майбутньому.

Дослідження теми організації захисту інформації дозволить виявити недоліки та можливості для їх покращення у сфері кібербезпеки. Враховуючи важливість права на інформацію для громадян та підприємств, нормативно-правова база України має враховувати засади забезпечення інформаційної безпеки, зокрема, правила та процедури висвітлення діяльності органів влади та місцевого самоврядування, які зберігають конфіденційну інформацію. Такий підхід дозволяє забезпечити безпеку інформації та захист важливих національних інтересів.

У боротьбі за свободу, незалежність та збереження національного суверенітету, інформаційна безпека стає ключовим фактором, що визначає успіх

чи невдачу. Від здатності держави і суспільства захищати свою інформацію, критичну інфраструктуру, та ефективно протистояти інформаційним атакам, залежить їхнє стійке функціонування та здатність забезпечити безпеку та благополуччя своїх громадян. Отже, організація захисту інформації залишається надзвичайно актуальною в сучасних умовах, і вивчення цієї теми має велике значення для забезпечення інформаційної безпеки та стабільності в Україні.

У наукових публікаціях значна увага приділялася визначенню таких понять, як інформаційна безпека, безпека інформації та кібербезпека. В літературі висловлюється думка, що інформаційна безпека – це стан захищеності систем та даних. Вона стосується фізичного захисту інформації та його матеріального носія. Захист інформації – це сукупність методів і засобів, для забезпечення саме інформаційної безпеки, тобто теоретико-практична частина цієї сфери. Кібербезпека – це частина інформаційної безпеки, яка спрямована на захист сучасних комп'ютерних технологій [36]. В інформаційному суспільстві кібербезпека набуває неабиякої ваги та актуальності. Тому в контексті кваліфікаційній роботі досліджується як захист інформації в кіберпросторі, так і організація системи захисту інформації на різних носіях в Секретаріату Кабінету Міністрів України використовуються усі аспекти інформаційної безпеки.

Актуальність теми обумовлює й інтерес до неї у наукових колах. Процеси інформаційної безпеки центральних органів влади досліджували такі науковці, як Ткачук Т. [69], Войціховський А. [29], Панченка О. [59], Гаврильців М. [32], Левченка О. В.[50], Шемчук В.В. [73] та інші.

Зв'язок з науковими програмами, планами і темами. Матеріал для написання кваліфікаційної роботи збирався на базі Секретаріату Кабінету Міністрів України.

Мета дослідження полягає в узагальнені знань щодо інформаційної безпеки в Україні та в Секретаріаті Кабінету Міністрів України. Мета передбачає **завдання**:

– розглянути стан дослідження теми в науковій літературі та джерелах;

– проаналізувати нормативно-правову базу інформаційної безпеки в Україні та її основні складові;

– охарактеризувати роль захисту інформації в діяльності установ та організацій;

– визначити систему захисту інформації в Секретаріаті КМУ;

– розкрити роль партнерства у сфері захисту інформації.

Об'єктом дослідження є захист інформації в органах виконавчої влади України**.**

Предметом дослідження є специфіка організації інформаційної безпеки в Секретаріаті КМУ, безпека інформації в кіберпросторі.

Методологічну основу даної роботи складають сукупність загальнонаукових принципів і підходів, а також спеціально-наукових методів пізнання, які допомогли отримати науково обґрунтовані результати. Використовувалися такі методи аналізу та синтезу, історичний метод, метод бібліографічної евристики та метод узагальнення.

Новизна дослідження в полягає в узагальнені досвіду організації захисту інформації в Секретаріаті Кабінету Міністрів України.

Практичне значення одержаних результатів. Матеріал кваліфікаційної роботи можна використати для поліпшення обізнаності в сфері інформаційної безпеки та подальшого вдосконалення навчальних програм, таких дисциплін як «Державна інформаційна політика», «Електроне урядування».

Особистий внесок. Кваліфікаційна робота виконана самостійно. Всі основні результати дослідження належать авторові особисто.

Апробація результатів. Ключові положення кваліфікаційної роботи доповідалися на XXIII Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки» (м. Київ, 6 квітня 2023 року).

Публікації. Слюсар І.В. Інформаційна безпека України: сучасний стан та перспективи. «Політ. Сучасні проблеми науки». Гуманітарні науки: тези

доповідей XXIII Міжнародної науково-практичної конференції молодих учених і студентів. Київ: НАУ, 2023, С. 190–191.

Структура кваліфікаційної роботи. Кваліфікаційна складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Список джерел налічує 80 найменування. Загальний обсяг роботи – 109 сторінок (без додатків).

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

1.1. Аналіз наукової літератури та джерел

Тема інформаційної безпеки України надзвичайно актуальна в сучасному світі, оскільки країна стикається з численними викликами і загрозами. Зокрема, в контексті збройних конфліктів та гібридної війни на власній території, спровокованих російсько-українським конфліктом, Україна постійно стикається з деструктивним інформаційним впливом, який наносить значні збитки державі та суспільству. Ці виклики змушують багатьох вчених та фахівців працювати над розробкою та впровадженням ефективних стратегій і систем забезпечення інформаційної безпеки, щоб забезпечити надійний захист національних інтересів та збереження суверенітету країни. Аналізуючи наукові статті можна виділити декілька напрямів наукових досліджень.

Дослідження, присвячені вивченню сутності інформаційної безпеки та її взаємозв'язку з національною безпекою. Зокрема, поняття «інформаційна безпека» розглядався в науковій та законодавчій площині [додаток А].

У статті Войціховського А. «Кібербезпека як важлива складова системи захисту національної безпеки європейських країн» (2018 р.), досліджується важливість кібербезпеки як необхідного компонента для забезпечення національної безпеки в Європі. В рамках статті проводиться аналіз передумов і особливостей формування законодавства України в галузі кібербезпеки на основі європейського досвіду, а також визначаються проблеми та перспективи подальшого розвитку цього законодавства з урахуванням оцінки наявних небезпек і загроз [30]. Також автор розглянув шляхи адаптації чинного законодавства щодо кібербезпеки в Україні до стандартів Європейського Союзу в рамках виконання положень Угоди про асоціацію між Україною та ЄС. Автор

аналізував досвід європейських країн у сфері законодавчого забезпечення кібербезпеки та довів доцільність розвитку договірного державно-приватного партнерства в сфері захисту кіберпростору.

Колектив авторів (Біленчук П., Борисова Л., Неклонський І. та Собина В.) у монографії «Правові засади інформаційної безпеки України» (2018 р.), систематизував матеріал про інформаційну безпеку на різних рівнях: від індивідуального до державного. У публікації детально розглянуті особливості інформації як об'єкта правового регулювання в контексті інформаційної безпеки та питання юридичної відповідальності за порушення правових норм [25]. Автори привернули увагу на важливість інформаційної безпеки для захисту прав та інтересів громадян, суспільства та держави. Вони дослідили не лише технічні аспекти інформаційної безпеки, а й її правові засади. Автори запропонували шляхи та рекомендації щодо покращення правового регулювання в цій сфері. У монографії був зроблений широкий огляд сучасних проблем і викликів, що виникли у зв'язку з розвитком інформаційних технологій і їх впливом на безпеку інформації, досліджені питання юридичної відповідальності за порушення правових норм у сфері інформаційної безпеки.

У статті Антонова С. та Г. Мартинюк Г. «Інформаційна безпека» (2019р). було проаналізовано теоретичні аспекти інформаційної безпеки з позицій різних дослідників. Проведений аналіз літературних джерел дозволив авторам виявити та систематизувати рівні організаційної системи забезпечення інформаційної безпеки держави. Вони також акцентували увагу на основних завданнях державної інформаційної політики та узагальнено періодизацію розвитку державного управління забезпеченням інформаційної безпеки. Зазначили, що розвиток системи державного управління забезпеченням інформаційної безпеки України проходив у чотири етапи, кожний з яких характеризується своїми пріоритетами, проблемами, шляхами їх вирішення та тривалістю. Показали позиції України в світовому рейтингу країн з найбільшими ризиками в інформаційній сфері та зазначені основні тенденції, пов'язані із виявленими

загрозами. Систематизували колишні недоліки державної інформаційної політики України в сучасних умовах, що пов'язаних із недосконалістю нормативно-правової бази, відсутністю ефективної державної політики, недостатністю розвиненості національної інформаційно-комунікаційної інфраструктури, значною кількістю застарілих телекомунікаційних мереж. Обґрунтували необхідність посилення впливу органів державної влади щодо ліквідації проблем, пов'язаних із покращенням інформатизації суспільства та забезпеченні належної інтеграції українського інформаційного простору в європейський [22].

У статті «Інформаційна складова національної безпеки» автора Панченка О. (2019 р.), акцентується увага на інформаційній безпеці як важливій складовій національної безпеки. У цій роботі надаються визначення понять «інформаційна безпека» та «національна безпека» і розглядаються аспекти інформаційної безпеки в умовах розвитку інформаційного суспільства та інформатизації [59]. Панченко О. провів аналіз впливу загальних підходів до організації інформаційної безпеки на систему національної безпеки держави. Він звернув увагу на той факт, що в сучасному світі інформація стала важливим ресурсом і об'єктом впливу з боку зовнішніх суб'єктів. Автор розглядає загрози, пов'язані з інформаційною безпекою, такі як кібератаки, кібершпигунство, маніпуляція інформацією та дезінформація. У статті також досліджується важливість забезпечення інформаційної безпеки для національної безпеки держави. Автор наголошує на необхідності розроблення ефективних стратегій, політик та механізмів захисту інформаційної інфраструктури держави. Він підкреслює важливість підвищення кваліфікації та освіти в галузі інформаційної безпеки, а також співпраці з іншими країнами для обміну досвідом та спільних заходів забезпечення інформаційної безпеки. Загалом, у статті розглядається інформаційна безпека як важливий аспект національної безпеки та пропонуються різноманітні підходи і рекомендації для забезпечення ефективного захисту інформаційних ресурсів та інфраструктури держави.

У статті авторів Довгань О. та Ткачук Т. «Концептуальні засади законодавчого забезпечення інформаційної безпеки України» (2019р.) розглянуто концептуальні засади правового забезпечення інформаційної безпеки України. В ході дослідження вони проводять теоретичний аналіз, результатом якого є запропонована модель Закону України «Про інформаційну безпеку України». Додатково в статті ретельно аналізуються та розглядаються основні складові цього законопроекту. Робота авторів спрямована на вивчення та уточнення концепції інформаційної безпеки в контексті України, а також на розробку моделі законодавчого акту, який би враховував специфіку цієї галузі та забезпечував необхідний правовий фундамент для зміцнення інформаційної безпеки в країні [44].

Стаття Гаврильціва М. «Інформаційна безпека держави у системі національної безпеки України» (2020 р.) присвячена розгляду інформаційної безпеки як важливої складової національної безпеки в Україні в умовах гібридної війни [32]. У статті підкреслено, що в Україні станом на 2020 р. практично відсутня система інформаційної безпеки, яка б могла ефективно виявляти та аналізувати інформаційні загрози національній безпеці та протидіяти їм. В умовах гібридної війни інформаційна складова стала об’єктом маніпуляцій, оскільки складна політична ситуація в країні та постійне погіршення іміджу на міжнародній арені створюються через недостатній рівень інформаційної безпеки. Забезпечення інформаційної безпеки стає необхідною складовою національної безпеки України. Автором статті визначені основні елементи інформаційної безпеки, серед яких інформування громадян, вільний доступ до різних джерел інформації та захист від негативних впливів фейкових новин та дезінформації. У статті підкреслено, що реалізація національної інформаційної стратегії сприяє у забезпеченні інформаційної безпеки та успішному вирішенні завдань у різних сферах державної діяльності, включаючи політичну, військовополітичну, соціальну та економічну сфери. Вдала інформаційна політика може суттєво вплинути на вирішення внутрішньополітичних,

зовнішньополітичних та військових конфліктів. У статті підкреслено, що система інформаційної безпеки держави є необхідною складовою загальної системи національної безпеки, і вона повинна забезпечуватись узгодженою діяльністю органів державної влади, недержавних структур та громадян на основі єдиних правових норм. Тільки такий підхід може ефективно протистояти інформаційним загрозам в сучасних умовах.

Метою статті Сопілки І., «Інформаційна безпека та кібербезпека: порівняльно-правовий аспект» (2021р.), ознак та сутності кібербезпеки та інформаційної безпеки та проведення їх порівняльно-правового аналізу. Автор розібрала поняття, сутність, характеристики кібербезпеки та інформаційної безпеки, зазначила проблеми забезпечення їх функціонування, надала рекомендації щодо подолання таких проблем шляхом вдосконалення чинної законодавчої бази та гармонізації національного законодавства з міжнародними стандартами [66].

Дослідження, присвячені вивченню досвіду у сфері інформаційної безпеки.

У статті за авторством Вітер С. та Світлишин І. «Захист облікової інформації та кібербезпека підприємства» (2017 р.), розглядалися важливі аспекти забезпечення безпеки облікової інформації та кібербезпеки на підприємствах. В статті обґрунтовується актуальність питання організації системи кібербезпеки облікової інформації на підприємствах. Визначено принципи та заходи, спрямовані на забезпечення захисту облікової інформації в контексті кібербезпеки. Також авторами розглядаються деякі аспекти організації цього процесу та пропонується власне розуміння поняття «кібербезпека облікової інформації». [28]

Стаття «Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз» автора Ткачука Т. (2017 р.) присвячена огляду підходів до сутності загроз в інформаційній безпеці та політико-правовому аналізу таких загроз українській інформаційній безпеці на сучасному етапі [69]. Автор

проаналізував різні підходи до розуміння сутності загроз інформаційній безпеці. Він розглядав їх як складну систему, яка включає технологічні, організаційні, соціальні та правові аспекти. Зокрема, Трачук Т. підкреслив, що загрози інформаційній безпеці виявляються через незаконне використання інформаційних технологій, маніпулювання інформацією, кібератаки, дезінформацію та інші негативні явища, спрямовані на порушення безпеки інформаційного простору держави. Трачук Т. здійснив політико-правовий аналіз загроз інформаційній безпеці України на сучасному етапі. Автор наголосив на необхідності прийняття та удосконалення правових актів, спрямованих на запобігання та протидію загрозам інформаційній безпеці. Він зазначив, що правовий захист інформаційної безпеки має бути комплексним, враховувати міжнародні стандарти та норми, а також забезпечувати ефективний механізм протидії загрозам національній безпеці.

Крім того, Трачук Т. проаналізував конкретні загрози інформаційній безпеці України, такі як кіберзлочинність, кібершпигунство, дезінформація та маніпуляція інформацією. Автор підкреслив необхідність розвитку кіберзахисту, підвищення кваліфікації фахівців у галузі інформаційної безпеки та зміцнення міжнародного співробітництва в цій сфері.

Загалом, у статті здійснено детальний огляд загроз інформаційній безпеці та проведено їх політико-правовий аналіз. Автор підкреслив важливість прийняття правових заходів та застосування заходів для забезпечення інформаційної безпеки, щоб захистити національні інтереси та забезпечити стабільність і безпеку держави.

У статті Візир Т., «Адміністративно-правове регулювання забезпечення інформаційної безпеки в Україні: сучасний стан та перспективи вдосконалення» (2019р.) було досліджено сучасний стан адміністративно-правового регулювання забезпечення інформаційної безпеки в Україні. Виявлено низку проблем у вказаній сфері. Наведено комплекс рекомендацій щодо їх розв’язання.

Визначено напрями вдосконалення законодавства, що забезпечує адміністративно-правового регулювання інформаційної безпеки в Україні [27].

Автори Піддубна Л. та Павліченко В. у своїй статті «Інформаційна безпека в системах електронного документообігу» (2020р.) розглянули питання інформаційної безпеки в системах електронного документообігу. Вони визначали, що інформаційна безпека в системах електронного документообігу є комплексним завданням, вирішення якого потребує поєднання заходів на законодавчому, адміністративному, процедурному та програмно-технічному рівнях [63].

Стаття «Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід)» автора Войціховського А. (2020 р.) присвячена розгляду правових і організаційних основ забезпечення інформаційної безпеки держав у сучасному інформаційному суспільстві. У статті проведений аналіз теоретичних підходів до розуміння сутності «інформаційна безпека» та «національна безпека», а також встановлюється їх взаємозв'язок [29]. Автором також було розглянуто сучасні загрози інформаційній безпеці, такі як кіберзагрози, кібератаки, маніпуляція інформацією та дезінформація. Він вказав на необхідності розробки ефективних політико-правових механізмів і заходів забезпечення інформаційної безпеки, які відповідають сучасним викликам і загрозам. Загалом, стаття надала детальний аналіз теоретичних та практичних аспектів інформаційної безпеки в контексті національної безпеки. А у статті підкреслено важливість розробки ефективних стратегій, політик і заходів забезпечення інформаційної безпеки для захисту національних інтересів, стабільності і розвитку держави у сучасному інформаційному суспільстві.

У статті Яковлєва П. «Об'єкт і предмет державного регулювання у сфері забезпечення інформаційної безпеки України» (2020р.), розкривається зміст і пропонується авторський варіант тлумачення таких категорій, як об'єкт і предмет державного регулювання у сфері забезпечення інформаційної безпеки

України. Об’єктом державного регулювання у сфері забезпечення інформаційної безпеки запропоновано вважати суспільні відносини, які формуються у процесі державно-владної діяльності уповноважених органів управління, спрямованої на забезпечення життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. Зазначено, що як інтереси особи в інформаційній сфері, так і інтереси суспільства та держави визначаються здебільшого актуальними загрозами, а також ступенем впровадження досягнень глобального і національного технічного прогресу у сфері формування й оперування інформаційними даними [79].

У статті Чалапко В., «Іінформаційна безпека: до проблеми місця й ролі у системі національної безпеки» (2021р.), обґрунтовується, що здійснюваний інформаційний вплив за допомогою технологій контролю і маніпулювання суспільною свідомістю викликає дисфункційні процеси, що перешкоджають оптимальному функціонуванню державних інститутів. Основним об’єктом захисту у даному випадку виступає суспільна свідомість. Зазначається, що специфіка інформаційної безпеки дозволяє їй охопити всі види безпеки: економічну, соціально-політичну, військову та екологічну, тому її забезпечення є пріоритетним завданням у процесі вирішення проблем національної безпеки. Від забезпечення інформаційної безпеки на сучасному етапі розвитку суспільства залежать умови забезпечення основних видів безпеки держави [72].

Публікації, присвячені вивченню вітчизняного досвіду у сфері інформаційної безпеки після початку війни.

У статті Валюшко І. «Інформаційна безпека України: трансформація законодавства після російського вторгнення» (2017 р.) [26], розглянуто важливі зміни в законодавстві України в галузі інформаційної політики, що було пов’язано з російською військовою агресією проти України. Важливо було усунути прогалини у законодавчій базі України, посилити протистояння зовнішнім (російським) інформаційним впливам у контексті гібридної війни. У статті зазначено, що деякі концептуальні документи, такі як воєнна доктрина,

були прийняті в останні рок з урахуванням сучасної безпекової ситуації та перспективи можливого приєднання України до військово-політичного союзу НАТО. Також акцентується увага на співпраці України з країнами ЄС та НАТО в інформаційно-військовій сфері у новоприйнятих концептуальних документах [10]. У статті проаналізовано законодавство, яке спрямоване на обмеження або заборону використання інформаційного контенту країни-агресора на радіо, телебаченні та в інтернет-просторі України. Водночас відзначається, що формування законодавства у цій сфері здійснюється за принципом надолуження згаяного, що залишається основною проблемою у сфері безпеки. Авторка підкреслила важливість стратегічного планування та прогнозування інформаційної та безпекової політики країни.

У статті «Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи» автора Шемчука В. (2019 р.) досліджувалися теоретичні основи та законодавче забезпечення понять «інформаційна безпека» та «інформаційна оборона». У статті проаналізовано практику та різні підходи до розуміння сутності інформаційної безпеки як у юридичній науці, так і в інших галузях української науки [74]. Автор звернув увагу на термінологічну невизначеність та різні підходи до розуміння інформаційної безпеки. Він розглянув інформаційну безпеку як стан захищеності інформаційного простору та підкреслив її важливість як частини державної політики у сфері національної безпеки і оборони. Аналізуючи положення Конституції України та ряду законів, Шемчук В. показав, що інформаційна безпека є одним із напрямів державної політики у сфері національної безпеки і оборони. Автор дослідив поняття «інформаційна оборона» як системи заходів захисту інформаційної та віртуальної сфери. Завдання інформаційної оборони включають готовність до інформаційного впливу та нападів з боку інших держав, захист і розвиток інформаційного простору, підвищення обороноздатності Збройних Сил та цивільного населення від інформаційних атак. Шемчук В. зазначив, що в Україні на законодавчому рівні визначено

повноваження державних органів у сферах національної безпеки і оборони, систему командування, контролю та координації операцій сил безпеки й сил оборони. У статті підкреслена взаємозалежність та взаємодоповнюваність понять «інформаційна безпека» та «інформаційна оборона» і спрямованість їх на забезпечення захищеності інформаційного простору, впровадження превентивних і захисних заходів, усунення інформаційних загроз та безпечний розвиток національного інформаційного простору [74].

Монографія Левченка О. «Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування» (2021 р.), є важливою з огляду організацію надійного захисту інформації України в умовах гібридної війни та інформаційних загроз, створених внаслідок російської агресії [50]. У цій монографії автор зосередився на методології побудови та функціонування системи забезпечення інформаційної безпеки в воєнній сфері. Автор проаналізував досвід і результати своєї практичної роботи в цій галузі та запропонував концепцію, яка базується на розробленій ним методології. Левченко О. запропонував практичні рекомендації для розвитку цієї системи. Монографія О. Левченка є важливим внеском у дослідження інформаційної безпеки України в умовах воєнної сфери. Його методологія та рекомендації становлять практичний інструмент для розробки ефективних заходів забезпечення інформаційної безпеки держави.

Стаття Залєвської І. та Удренас Г. «Інформаційна безпека України в умовах російської військової агресії» (2022 р.), присвячена питанням стану інформаційної безпеки України в контексті російської військової агресії [45]. Автори відзначили, що національні інтереси України вимагають створення сприятливих умов для політичного розвитку країни. Інтереси громадян включають в себе захист їхніх політичних прав і свобод. Суспільство потребує зміцнення демократії, а інтереси держави визначаються необхідністю ефективного захисту конституційного ладу, суверенітету та територіальної цілісності країни, а також забезпечення політичної стабільності, включаючи

стабільність державної влади та її інститутів. У цьому контексті інформаційна політика стає важливим інструментом для досягнення національних цілей. Автори наголосили, що ефективна інформаційна діяльність може суттєво покращити зусилля держави щодо мирного вирішення кризових ситуацій. Протилежність інформаційних чинників та надмірне спотворення інформації можуть спровокувати ворожість та мати серйозні наслідки. Автори також розглядають важливість використання інформаційних технологій у військовій сфері та контролю над інформаційними ресурсами. Це стає необхідним атрибутом для забезпечення оборони держави, і перевага в інформаційному протистоянні може сприяти досягненню стратегічних цілей країни. Сама Стратегія інформаційної безпеки України, на думку дослідників, відображає інтереси держави, зокрема, захист конституційного ладу, суверенітету та територіальної цілісності, підтримку політичної стабільності та державної влади. Аналіз її реалізації показує, що цей процес не зупиняється, навіть у складних умовах воєнного стану. Отже, у статті висвітлені актуальні питання інформаційної безпеки України в умовах російської військової агресії та підкреслено важливість ефективного захисту національних інтересів, досягнення стратегічних цілей і застосування інформаційних технологій у військовій сфері.

Стаття Котерліна І. «Інформаційна безпека в умовах воєнного стану в аспекті забезпечення інформаційних прав та свобод» (2022 р.) присвячена питанням побудови дієвої інформаційної політики як стратегічного інструменту перемоги в сучасних воєнних умовах [49]. Автор підкреслив, що інформація має величезний вплив на внутрішні протиріччя та може бути використана для досягнення перемоги без активного використання зброї. Якісна державна інформаційна політика може сприяти досягненню тактичних, оперативних і стратегічних цілей держави. Водночас у статті підкреслено, що в умовах, коли кожен громадянин може стати джерелом інформації і лідером суспільної думки, поширювана інформація не завжди відповідає потребам захисту національної безпеки. Автор висловив думку, що регулювання питань інформаційної безпеки

має здійснюватися шляхом правового регулювання. Проте важливо залишати пріоритетними демократичні права і свободи громадян, навіть у воєнний період. У статті розглянуті різні аспекти забезпечення інформаційних прав та свобод в контексті захисту інформаційної безпеки держави під час воєнного стану. Автор наголосив на пріоритетних напрямках захисту та впливу на права та свободи людини і громадянина. Важливим є збереження правових принципів для майбутнього відновлення держави на демократичних засадах. Отже, забезпечення інформаційної безпеки вимагає комплексного підходу, включаючи правові, політичні і технічні аспекти. Необхідно створити механізм, який ефективно регулюватиме інформаційні обмеження, а водночас забезпечуватиме захист прав і свобод громадян.

У статті Новицького В. «Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах» авторства (2022 р.) розглянуті гібридні інформаційні загрози з боку російського агресора, і виклики, які стоять перед Україною [48]. У статті проаналізовано основні положення сучасної Стратегії інформаційної безпеки України, висвітлено її зміст, мету та завдання. Зокрема, розглянуті концептуальні засади державної інформаційної політики в умовах сучасності і типові види загроз зовнішнього інформаційного впливу. У статті приділено особливу увагу особливостям проведення спеціальних інформаційних операцій проти України. Автор проаналізував стратегічні засади забезпечення інформаційної безпеки та підсумував досягнення вітчизняних спецслужб у цій сфері. Також Новицький В. уточнив компетенції вітчизняних спецслужб щодо забезпечення інформаційної безпеки в умовах реформування безпекової системи. У статті також визначені шляхи подальшої діяльності СБУ в рамках реалізації контррозвідувальних та оперативно-розшукових заходів, спрямованих на запобігання та локалізацію деструктивної діяльності російського агресора, спрямованих на підрив державних інтересів України в інформаційній сфері [55].

У статті Мазепи С. «Інформаційна безпека в умовах війни» (2022 р.) проаналізовано вплив інформаційного продукту, який поширюється за

допомогою засобів масової інформації, на свідомість суспільства та окремих груп у контексті російсько-української війни [54]. У статті відзначено, що пропаганда та розповсюдження недостовірної інформації становлять загрозу національній безпеці і можуть спонукати до прийняття помилкових рішень або навіть злочинних дій. Мазепа С. вказав на необхідність систематизації видів протиправної пропаганди, які є найбільшою загрозою суспільству, та притягнення до кримінальної відповідальності за такі дії. Аналізуючи зміни до Кримінального кодексу України, внесені внаслідок російської військової агресії проти України, автор зупинився на аналізі на статті 111-1 «Колабораційна діяльність», яка включає різні склади злочинів. Зокрема, в статті вказується на протиправну пропаганду в закладах освіти з метою сприяння збройній агресії проти України та уникнення відповідальності за збройну агресію. Автор статті підкреслює, що протиправна пропаганда включає такі прояви, як пропаганда культури насильства, війни, наркотиків, екстремізму та тероризму. Розробка і впровадження методики збору та оброблення даних кіберстатистики має на меті оптимізацію процесів забезпечення кібербезпеки та зміцнення інформаційної безпеки в Україні, що стає дедалі важливішою завданням в умовах сучасного цифрового середовища.

У статті Ткаченко В. та Паливоди В «Загрози інформаційній безпеці України як проблематика національної безпеки», (2022 р.), аналіз був зосереджений на важливих аспектах інформаційної безпеки України в контексті російсько-українського конфлікту. Стаття відзначала, що цей конфлікт включає не лише військові дії, але і інформаційний аспект, що робить його гібридним. Автори статті наголошують на тому, що російська агресія включає в себе інформаційну пропаганду та використання інформаційних технологій для досягнення політичних цілей. Аналізуючи стан інформаційної безпеки України, автори вказують на важливість протидії кіберзлочинності. Вони зазначають, що багато кіберзлочинів залишаються невиявленими, і що ця проблема потребує систематизації та розв’язання. В статті було проаналізовано перелік загроз

інформаційній безпеці України в контексті російсько-українського конфлікту що дає цінний внесок у розуміння цієї проблеми. Автори визначають напрямки вирішення цих загроз та шляхи для протидії інформаційним загрозам національній безпеці України [70].

У статті Гончарова М. «Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України» (2022 р.), було розглянуто концептуальні засади нормативно-правового забезпечення інформаційної безпеки в Україні з позицій різних дослідників. Проведений аналіз наукових джерел дозволив виявити, що нормативно-правове забезпечення інформаційної безпеки в цілому, так і на елементному рівні характеризується науковістю, системністю та має багато аспектів [33].

У статті Невельської-Гордєєвої О. «Феномен «fake news» в контексті забезпечення інформаційної безпеки держави» (2022р.), аналіз автора був присвячений дослідженню основних моментів використання «fake news» для маніпуляцій масовою свідомістю з метою інформаційно-психологічного впливу. «Fake news» розглядається як прихований вплив. Інформаційне вторгнення, маніпуляції, застосування соціально-психологічного впливу є серйозною загрозою як головним засадам демократичного суспільства, так і особистій інформаційно-психологічній безпеці громадян [56].

Колектив авторів (Давидюк А. Зубок В, Хохлачова Ю., Худинцев М., Комаров М.) у статті «Кіберстатистика в Україні: сучасний стан» (2023р.) дослідив актуальну проблематику кіберстатистики в контексті України. В ході дослідження вони аналізують розвиток кіберзахисту в країні та звертають увагу на зростаючі технічні можливості для забезпечення безпеки інформації. Автори висвітлюють, що новітнє обладнання може збирати значні обсяги даних для подальшого аналізу потенційних кіберзагроз. У цьому контексті автори роблять акцент на важливості впровадження процесів кіберстатистики, які допоможуть відрізняти функції різних суб’єктів, які працюють у сфері кібербезпеки, на основі використаних наборів даних. Ця диференціація сприятиме виявленню проблем у

діяльності цих суб’єктів та сприятиме впровадженню уніфікованих підходів до збору та аналізу даних в галузі кібербезпеки. [43]

У статті Виздрика В, «Інформаційна безпека в Україні: сучасний стан» (2023р,) проводиться аналіз присвячений сучасному стану інформаційної безпеки, яка є необхідною для життєво важливих інтересів людини і громадянина встановлюється взаємозв’язок між війною і політикою в сучасних умовах. Автором зазначено що інформаційна безпека зумовлена насамперед стрімким зростанням технічних можливостей сучасних інформаційних систем, вплив яких є визначальним і всеосяжним на політичне, економічне життя, духовну та ідеологічну сфери людей. У сучасних умовах інформаційна безпека стає найважливішим базовим елементом системи національної безпеки України [31].

У статті Шульженко Н. «Інформаційна безпека від загроз транснаціональної організованої злочинності» (2023р) здійснений аналіз був присвячений дослідженню інформаційної безпеки від загроз транснаціональної організованої злочинності. Організована злочинність становить потенційну та основну загрозу національній безпеці нашої держави. Актуальність теми дослідження визначається тим, що транснаціональна організована злочинність є не лише потенційною, а й реальною загрозою національній безпеці, державному суверенітетові, забезпеченню прав та свобод людини та громадянина. Транснаціональна злочинність є явищем, яке не тільки не обмежується кордонами однієї держави, а й впливає на глобальну безпеку людства [75].

У процесі дослідження теми магістерської кваліфікаційної роботи вивчався блок джерел, у який увійшли законодавчі та нормативно-правові документи, документи КМУ з питань захисту інформації. Законодавча та нормативно-правова база захисту інформації в Україні полягає в наступних пунктах законів, які регулюють сферу захисту інформації, або своїм існуванням якось впливають на процес діяльності в цій сфері, наприклад укази, які

встановлюють законність військового стану. Були розглянуті наступні нормативно-правові документи:

Конституція України – є основним законом України, в якому зазначено низку положень, що стосуються життя в державі, в тому числі і інформаційної безпеки країни. Зокрема, у ст. 17 Конституції України передбачено право на недоторканість житла, кореспонденції, телефонних розмов та інших засобів комунікації. Це означає, що держава зобов'язана захищати конфіденційність інформації, яка передається через ці засоби комунікації [1]. Крім того, ст. 32 Конституції України передбачає право на вільний доступ до інформації, що належить до відкритих джерел. Держава зобов'язана забезпечувати відкритість діяльності органів державної влади та місцевого самоврядування, забезпечувати доступ до документів та інформації про діяльність цих органів [1].

Ст. 49 Конституції України передбачає право на захист від незаконного втручання у приватне життя, особисту та сімейну таємницю. Це означає, що держава зобов'язана захищати від будь-яких спроб порушення приватності громадян, зокрема, через незаконне збирання, зберігання та використання їхньої персональної інформації [1].

Також Конституція України передбачає право на свободу думки та совісті, а також право на інформацію. Проте ці права можуть бути обмежені у випадках, коли це необхідно для захисту національної безпеки, громадського порядку, здоров'я та моралі населення. Таким чином, у Конституції України акцентується на важливості захисту інформаційної безпеки та приватності громадян, на важливості захисту конфіденційної інформації, а також створенні правової базу для регулювання цих питань у відповідних законах та нормативно-правових актах.

Реалізація прав громадян та інформаційної безпеки держави регулюється у відповідних законах та нормативно-правових актах. Зокрема, Україна має закони, що стосуються інформаційної безпеки, такі як Закон України «Про захист персональних даних», Закон України «Про інформацію», Закон України

«Про електронні довірчі послуги», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та інші. До того ж, держава зобов'язана регулювати діяльність органів державної влади, що мають доступ до конфіденційної інформації, а також контролювати дотримання законодавства з питань захисту інформації у приватному секторі.

Закон України «Про інформацію», ухвалений 02 жовтня 1992 р. [2] є одним з основних законодавчих актів, які регулюють збір, зберігання, обробку, використання, поширення та захист інформації в Україні. Цей закон містить важливі положення про захист інформації від несанкціонованого доступу, використання та розголошення, а також про обов'язки органів державної влади, бізнесу та громадян щодо забезпечення інформаційної безпеки. Закон визначає правову базу щодо регулювання обігу інформації в Україні, а також передбачає встановлення механізмів забезпечення конфіденційності, цілісності та доступності інформації. Крім того, він встановлює обов'язки суб'єктів інформаційних відносин щодо забезпечення інформаційної безпеки та відповідальність за їх невиконання [2]. Закон також містить положення про захист інформації, що становить державну таємницю, та встановлює процедури збору, зберігання, обробки та передачі такої інформації. Він також визначає права та обов'язки суб'єктів, які мають доступ до державної таємниці, та передбачає механізми захисту цієї інформації від несанкціонованого доступу.

Закон України «Про інформацію» є важливим компонентом нормативно-правової бази інформаційної безпеки в Україні та відображає принципи захисту інформації. Він визначає права і обов'язки суб'єктів інформаційних відносин, встановлює право громадян України на доступ до інформації, що належить до відкритих джерел, а також право на захист від незаконного втручання у приватне життя, особисту і сімейну таємницю. Законом визначені обов'язки органів державної влади та органів місцевого самоврядування щодо забезпечення інформаційної безпеки. Зокрема, органи державної влади та органи місцевого самоврядування відповідно до Закону зобов'язані:

а) здійснювати контроль за обігом інформації;

б) забезпечувати захист інформації від несанкціонованого доступу, використання та розголошення;

в) впроваджувати механізми захисту інформації, що становить державну таємницю;

г) проводити навчання з питань інформаційної безпеки [2].

Закон України «Про інформацію» є важливим інструментом захисту прав громадян України на інформацію та сприяє забезпеченню інформаційної безпеки України.

Закон України «Про електронні документи та електронний документообіг» [8] встановлює правові та організаційні основи електронного документообігу в Україні. Він регулює права та обов'язки суб'єктів електронного документообігу, встановлює порядок створення, зберігання, обробки, передачі та використання електронних документів, а також визначає відповідальність за порушення законодавства про електронний документообіг. Закон був прийнятий 22 травня 2003 року і є одним із найважливіших законів України в сфері електронного документообігу. Основні принципи електронного документообігу:

а) електронний документ має юридичну силу, якщо він відповідає вимогам закону і містить усі необхідні реквізити;

б) електронний документ може бути створений, переданий, збережений та оброблений з використанням електронних засобів;

в) електронний документ може бути підписаний електронним підписом;

г) електронний документ може бути визнаний недійсним, якщо він не відповідає вимогам закону або якщо він був підроблений;

Закон також встановлює порядок створення, зберігання, обробки, передачі та використання електронних документів. Відповідно до Закону електронні документи можуть створюватися, зберігатися, оброблятися та передаватися з використанням електронних засобів, а електронні документи можуть бути

підписані електронним підписом. Закон визначає відповідальність за порушення законодавства про електронний документообіг, зокрема, у вигляді штрафів або інші санкцій.

Закон «Про електронні документи та електронний документообіг» є важливим інструментом забезпечення інформаційної безпеки України. Закон сприяє підвищенню рівня захищеності електронних документів від несанкціонованого доступу, використання та розголошення. Закон також сприяє розвитку електронного документообігу в Україні, що позитивно впливає на ефективність роботи органів державної влади та органів місцевого самоврядування, а також бізнесу.

Закон України «Про основні засади забезпечення кібербезпеки України» (05 жовтня 2017 р.) [5] є важливим елементом нормативно-правової бази України в галузі інформаційної безпеки, оскільки він встановлює вимоги щодо захисту інформації в кіберпросторі, визначає обов'язки і права державних органів та суб'єктів господарювання щодо забезпечення кібербезпеки, а також передбачає механізми реагування на кібератаки та інші кіберзлочини. Закон містить вимоги щодо захисту критичної інфраструктури, систем, мереж та інших об'єктів, що мають важливе значення для національної безпеки. Також він встановлює обов'язок забезпечення захисту персональних даних та конфіденційної інформації.

Закон передбачає утворення координаційного центру з кібербезпеки, який має відповідати за координацію дій державних органів у галузі кібербезпеки та взаємодію з міжнародними структурами в цій сфері. Окрім цього, законом передбачено кримінальну відповідальність за кіберзлочини та порядок проведення розслідувань у цій сфері. В цілому, Закон має важливе значення для забезпечення інформаційної безпеки України в кіберпросторі та визначає необхідні заходи для запобігання кіберзагроз та кібератак. Сфера дії Закону України «Про основні засади забезпечення кібербезпеки України» спрямована на:

а) встановлення правових та організаційних основ забезпечення кібербезпеки України, що сприяє запобіганню кіберзагроз та кібератак;

б) визначення обов'язків суб'єктів інформаційних відносин щодо забезпечення кібербезпеки, що сприяє підвищенню рівня захищеності інформації від несанкціонованого доступу, використання та розголошення;

в) передбачення механізмів реагування на кібератаки та інші кіберзлочини, що сприяє відновленню нормального функціонування інформаційних систем та мереж після кібератак;

г) встановлення кримінальної відповідальності за кіберзлочини, що сприяє запобіганню кіберзлочинам та захисту прав громадян України на інформацію.

Закон України «Про основні засади забезпечення кібербезпеки України» є важливим інструментом забезпечення інформаційної безпеки України та сприяє підвищенню рівня захищеності інформації від несанкціонованого доступу, використання та розголошення.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 31 травня 2005 р, [3] має на меті захистити конфіденційну інформацію в інформаційно-телекомунікаційних системах (далі – ІТС) від несанкціонованого доступу, використання, зміни, знищення та поширення. Закон встановлює вимоги до захисту інформації та обов'язки суб'єктів господарювання, які мають доступ до такої інформації. Закон також встановлює вимоги до захисту інформації, що міститься в державних ІТС, і визначає порядок забезпечення безпеки інформації під час її оброблення в таких системах, під час її передачі через мережі зв'язку, включаючи інтернет. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» є важливим елементом нормативно-правової бази України в галузі інформаційної безпеки, оскільки встановлює вимоги щодо захисту конфіденційної інформації в ІТС та сприяє забезпеченню її безпеки в процесі оброблення та передачі.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» пов’язаний з захистом інформації в Україні у наступних аспектах:

а) встановлює правові та організаційні основи забезпечення захисту інформації в ІТС, що сприяє запобіганню несанкціонованому доступу, використанню, зміні, знищенню та поширенню інформації;

б) визначає обов’язки суб’єктів інформаційних відносин щодо забезпечення захисту інформації в ІТС, що сприяє підвищенню рівня захищеності інформації від несанкціонованого доступу, використання, зміни, знищення та поширення;

в) передбачає механізми реагування на несанкціонований доступ, використання, зміну, знищення та поширення інформації, що сприяє відновленню нормального функціонування ІТС після таких подій;

г) передбачає кримінальну відповідальність за несанкціонований доступ, використання, зміну, знищення та поширення інформації, що сприяє запобіганню таким діям та захисту прав громадян України на інформацію.

Отже, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» є важливим інструментом забезпечення інформаційної безпеки України та сприяє підвищенню рівня захищеності інформації від несанкціонованого доступу, використання, зміни, знищення та поширення.

Закон України «Про створення єдиної системи залучення, використання та моніторингу міжнародної технічної допомоги» (далі – Закон) був прийнятий 15 лютого 2002 року [4]. Він визначає правові, організаційні та фінансові засади залучення, використання та моніторингу міжнародної технічної допомоги в Україні. Створення єдиної системи залучення, використання та моніторингу міжнародної технічної допомоги складається з наступних елементів:

а) стратегічне планування – визначення пріоритетних напрямів та сфер використання міжнародної технічної допомоги.

б) залучення – отримання міжнародної технічної допомоги від донорів.

в) використання – ефективне використання міжнародної технічної допомоги для досягнення визначених цілей.

г) моніторинг – оцінка ефективності використання міжнародної технічної допомоги.

Організація захисту інформації в рамках єдиної системи залучення, використання та моніторингу міжнародної технічної допомоги передбачає:

а) забезпечення конфіденційності інформації про міжнародну технічну допомогу є важливим для захисту інтересів України та її партнерів. Наприклад, інформація про технічні характеристики оборонної техніки, яка надається Україні в рамках міжнародної технічної допомоги, повинна бути захищена від несанкціонованого доступу, використання, розголошення, модифікації чи знищення.

б) захист інформації від несанкціонованого доступу, використання, розголошення, модифікації чи знищення є важливим для забезпечення ефективності використання міжнародної технічної допомоги. Наприклад, інформація про результати реалізації проєктів міжнародної технічної допомоги повинна бути захищена від несанкціонованого доступу, використання, розголошення, модифікації чи знищення, щоб забезпечити можливість її використання для прийняття ефективних рішень.

в) забезпечення цілісності інформації про міжнародну технічну допомогу є важливим для забезпечення достовірності інформації, на основі якої приймаються рішення про залучення, використання та моніторинг міжнародної технічної допомоги. Наприклад, інформація про витрати, пов’язані з реалізацією проєктів міжнародної технічної допомоги, повинна бути захищена від несанкціонованих змін або знищення, щоб забезпечити достовірність звітності про результати реалізації цих проєктів.

Закон України «Про критичну інфраструктуру» 16 листопада 2021 р. [7] встановлює правові засади функціонування та захисту об’єктів критичної

інфраструктури України, що є важливими для забезпечення національної безпеки, економіки та соціального розвитку країни. Закон передбачає визначення та класифікацію об’єктів критичної інфраструктури, а також встановлює вимоги до їх захисту, що включає застосування сучасних засобів захисту інформації від кібератак та інших загроз.

Згідно з цим Законом, владні органи та оператори критичної інфраструктури повинні регулярно проводити аналіз ризиків, пов’язаних з функціонуванням та захистом об’єктів критичної інфраструктури, а також вживати заходів щодо запобігання та реагування на негативні наслідки в разі загроз або інцидентів. Отже, Закон України «Про критичну інфраструктуру» відображає важливість захисту критичних об’єктів інфраструктури від інформаційних загроз та кібератак, що безпосередньо впливає на забезпечення інформаційної безпеки України.

Закон України «Про критичну інфраструктуру» пов’язаний з організацією інформаційної безпеки України у наступних аспектах:

а) визначає правові та організаційні основи захисту критичної інфраструктури від інформаційних загроз та кібератак, що сприяє запобіганню таким загрозам та інцидентам;

б) встановлює обов’язки владних органів та операторів критичної інфраструктури щодо захисту критичної інфраструктури від інформаційних загроз та кібератак, що сприяє підвищенню рівня захищеності критичної інфраструктури від таких загроз та інцидентів;

в) передбачає механізми реагування на інформаційні загрози та кібератаки, що сприяє відновленню нормального функціонування критичної інфраструктури після таких загроз та інцидентів;

г) передбачає кримінальну відповідальність за кібератаки на об’єкти критичної інфраструктури, що сприяє запобіганню таким атакам та захисту прав громадян України на інформацію.

Закон України «Про критичну інфраструктуру» є важливим інструментом забезпечення інформаційної безпеки України та сприяє підвищенню рівня захищеності критичної інфраструктури від інформаційних загроз та кібератак.

Закон України «Про основи національної безпеки України» [11] визначає правові та організаційні основи забезпечення національної безпеки України. Закон встановлює основні принципи, завдання та напрями забезпечення національної безпеки України, права та обов'язки органів державної влади, інших державних органів та органів місцевого самоврядування, а також громадян України у сфері національної безпеки. Закон втратив чинності 08 липня 2018 р. Його замінив Закон України «Про національну безпеку України (21 червня 2018 року) [10], який визначив основи і принципи національної безпеки та оборони відповідно до Конституції України (статті 1, 2, 17, 18, 92), до мети та основних принципів державної політики, що мають забезпечити захист суспільства та прав громадян від загроз. Цим Законом чітко визначаються повноваження державних органів у галузі національної безпеки та оборони. Він також створює основу для інтеграції політики та процедур різних державних органів, чиї функції пов'язані з національною безпекою і обороною, а також визначає систему командування, контролю та координації операцій сил безпеки та сил оборони. Завдяки цьому Закону впроваджується комплексний підхід до планування у сферах національної безпеки та оборони, що забезпечує демократичний цивільний контроль над органами та структурами сектору безпеки та оборони. Закон визначив такі основні загрози інформаційній безпеці України:

а) підрив державного суверенітету, територіальної цілісності та недоторканості України;

б) порушення демократичного конституційного ладу, прав і свобод людини і громадянина;

в) дестабілізація суспільно-політичної та економічної ситуації в Україні;

г) заподіяння шкоди національним інтересам України в інформаційній сфері.

Закон визначив основні напрями забезпечення інформаційної безпеки України, зокрема:

а) створення ефективної системи захисту інформації;

б) підвищення рівня обізнаності суспільства з питань інформаційної безпеки;

в) розвиток інформаційних технологій і комунікацій;

г) співпраця з міжнародними організаціями у сфері інформаційної безпеки.

Різниця між Законом «Про національну безпеку України» та Законом «Про основи національної безпеки України» полягає в тому, що Закон «Про національну безпеку України» є більш всеосяжним і детальним документом, який визначає правові та організаційні основи забезпечення національної безпеки України в усіх сферах, зокрема в інформаційній сфері. Закон «Про основи національної безпеки України» був прийнятий у 1992 році і не враховував нових загроз, які виникли в інформаційній сфері в останні роки. Закон «Про національну безпеку України» був прийнятий у 2018 році і враховує нові загрози, зокрема загрози інформаційній безпеці України.

Закон України «Про правовий режим воєнного стану» 12 травня 2015 р. [12] визначає правові засади запровадження та функціонування воєнного стану в Україні або в окремих її місцевостях. Воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності. Законом передбачено, що в умовах воєнного стану:

а) органи державної влади, військове командування, військові адміністрації та органи місцевого самоврядування наділяються додатковими повноваженнями, необхідними для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності;

б) тимчасово, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

Ці обмеження можуть стосуватися:

а) пересування осіб і транспортних засобів;

б) роботи підприємств, установ і організацій;

в) проведення масових заходів;

г) користування радіоефірним простором;

д) доступу до інформації.

Зокрема, законом передбачено заборону:

а) виїзду з місць проживання осіб, які підлягають мобілізації;

б) зборів, мітингів, демонстрацій, інших масових заходів;

в) публікації матеріалів, що можуть завдати шкоди обороноздатності України;

г) використання засобів’язку та інформації для передачі інформації, яка може завдати шкоди обороноздатності України.

Таким чином, воєнний стан має значний вплив на організацію захисту інформації в Україні. У період воєнного стану органи державної влади, військове командування, військові адміністрації та органи місцевого самоврядування набувають додаткових повноважень у сфері захисту інформації. Зокрема, вони можуть:

а) заборонити або обмежити доступ до інформації, яка може бути використана ворогом;

б) здійснювати контроль за поширенням інформації;

в) забезпечувати інформаційну безпеку населення.

Крім того, в умовах воєнного стану громадяни та юридичні особи мають додаткові обов’язки щодо захисту інформації. Зокрема, вони повинні:

а) дотримуватися встановлених обмежень щодо поширення інформації;

б) забезпечувати безпеку інформації, яка їм довірена;

в) співпрацювати з органами державної влади, військовим командуванням, військовими адміністраціями та органами місцевого самоврядування у сфері захисту інформації.

Організація захисту інформації в умовах воєнного стану є важливим завданням, яке має бути вирішено для забезпечення національної безпеки України.

Указ президента України «Про введення воєнного стану в Україні» був запроваджений 24 лютого 2022 року в умовах повномасштабної російської військової агресії в сторону України. Воєнний стан був запроваджений на всій території України строком на 30 діб [16]. Основною метою введення воєнного стану було забезпечення національної безпеки та оборони України, усунення загрози небезпеки державній незалежності України, її територіальній цілісності та відсічі збройної агресії.

Указ передбачає ряд обмежень конституційних прав і свобод людини і громадянина, необхідних для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану. Зокрема, можуть обмежуватися:

а) свобода пересування;

б) свобода мирних зібрань;

в) право на свободу слова;

г) право на ведення підприємницької діяльності;

д) право на свободу пошти, телеграфу та телефонного зв’язку.

Указ також передбачає ряд заходів, які можуть бути запроваджені на період дії воєнного стану. Зокрема, можуть бути:

а) введені комендантська година;

б) введені обмеження на пересування громадян;

в) введені обмеження на переміщення товарів і вантажів;

г) введені обмеження на діяльність окремих підприємств і організацій.

Введення воєнного стану в Україні є надзвичайною мірою, яка застосовується в умовах загрози національній безпеці та обороні країни.

Постанова КМУ «Про затвердження Положення про державну службу спеціального зв'язку та захисту інформації України» від 3 вересня 2014 р. [6] є важливим документом, який регулює діяльність державної служби зі спеціального зв'язку та захисту інформації (далі – Держспецзв'язку). У Постанові визначені завдання та функції цієї служби, а також права та обов'язки її працівників. Згідно з Постановою, Держспецзв'язку здійснює заходи щодо захисту державної та іншої важливої інформації від несанкціонованого доступу, використання та поширення, а також забезпечує функціонування систем спеціального зв'язку та захисту інформації. Це важливо для забезпечення інформаційної безпеки України, оскільки державна та інша важлива інформація може бути цільовим об'єктом кібератак, шпигунства або інших загроз.

Положення про Держспецзв'язок встановлює, що ця служба взаємодіє з іншими органами державної влади, зокрема правоохоронними та військовими органами, з метою координації заходів з захисту інформації від зовнішніх та внутрішніх загроз. Крім того, Держспецзв'язку здійснює міжнародне співробітництво в галузі захисту інформації та бере участь у виконанні міжнародних договорів, укладених Україною з іншими країнами щодо захисту інформації. Таким чином, положення спрямоване на забезпечення інформаційної безпеки України шляхом координації дій між органами державної влади та міжнародним співробітництвом. Постанова сприяє зміцненню інформаційної безпеки України. Вона визначає правові та організаційні основи діяльності Держспецзв'язку, а також встановлює права та обов'язки її працівників, сприяє координації дій між органами державної влади та міжнародним співробітництвом у галузі захисту інформації, допомагає забезпечити інформаційну безпеку України та захистити державну та іншу важливу інформацію від несанкціонованого доступу, використання та поширення.

Постанова КМУ «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» від 24 березня 2023 р. регламентує процедуру проведення аудиту безпеки інформаційних технологій в організаціях незалежно від їх форм власності та галузі діяльності. Аудит виконується з метою виявлення та оцінки ризиків порушення безпеки інформації та розроблення рекомендацій щодо їх запобігання. Постановою був введений в дію Порядок, який встановив вимоги до проведення аудиту безпеки інформаційних технологій, включаючи забезпечення професійної компетентності аудиторів та застосування відповідних методів та інструментів. Крім того, постанова передбачає необхідність дотримання правил зберігання та обробки конфіденційної інформації, що стосується організації, яка проходить аудит [9].

Проведення аудиту безпеки інформаційних технологій є важливим інструментом забезпечення інформаційної безпеки України, оскільки дозволяє виявляти слабкі місця в системах захисту інформації та розробляти рекомендації щодо їх усунення. Застосування відповідних стандартів та методів при проведенні аудиту також сприяє підвищенню рівня кібербезпеки в Україні та забезпечує захист національної інформаційної інфраструктури від потенційних загроз.

Постанова «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» пов'язана з інформаційною безпекою України у наступних аспектах:

а) визначає правові та організаційні основи проведення аудиту безпеки інформаційних технологій в Україні, що сприяє запобіганню порушенням безпеки інформації та кібератакам;

б) встановлює обов'язки організацій щодо проведення аудиту безпеки інформаційних технологій, що сприяє підвищенню рівня захисту інформації в організаціях;

в) передбачає механізми реагування на порушення безпеки інформації та кібератаки, що сприяє відновленню нормального функціонування систем і мереж після таких порушень та атак;

г) передбачає кримінальну відповідальність за порушення безпеки інформації та кібератаки, що сприяє запобіганню таким діям та захисті прав громадян України на інформацію.

Постанова про проведення аудиту безпеки інформаційних технологій є важливим інструментом забезпечення інформаційної безпеки України та сприяє підвищенню рівня захисту інформації в Україні.

Указ Президента України «Про Стратегію інформаційної безпеки»(28 грудня 2021 р.) спрямований на зміцнення інформаційної безпеки в Україні. Основний зміст і ключові аспекти полягають:

а) у визначенні інформаційних загроз. Указ визначає загрози інформаційній безпеці України, зокрема, дезінформацію, пропаганду, кібератаки та інші дії, спрямовані на освіту інформації та дестабілізацію суспільства.

б) стратегія інформаційної безпеки. Указ встановлює загальну стратегію у сфері інформаційної безпеки, включаючи заходи щодо підвищення свідомості громадян, розвитку кіберзахисту, захисту критично важливих інфраструктур та боротьби з дезінформацією.

в) співпраця та координація. Указ закликає до співпраці з міжнародними партнерами у сфері інформаційної безпеки та створення спеціалізованих структур для координації дій в цій сфері.

г) фінансування. Документ визначає необхідність забезпечення фінансування програм і заходів, спрямованих на зміцнення інформаційної безпеки.

Загальна мета «Стратегії інформаційної безпеки» полягає в захисті суверенітету і національної безпеки України в інформаційному просторі, забезпеченні вільного доступу громадян до об’єктивної інформації та запобіганні маніпуляціям та дезінформації. Цей Указ відображає серйозний підхід уряду

України до забезпечення інформаційної безпеки та покликаний зміцнити захист від інформаційних загроз у сучасному світі [20].

Отже, аналіз літератури та джерел засвідчили, що питанням захисту інформації присвячено значний пласт наукових публікацій, а нормативно-правова база була значно оновлена та доповнена у зв'язку з російською воєнною агресією проти України.

1.2. Методи дослідження, які застосовувались при пошуку та роботі з джерелами

При дослідженні теми кваліфікаційної роботи застосовувались методи різних рівнів підпорядкування, що дозволило вирішити поставлені задачі. Зокрема, методи аналізу та синтезу дозволили ретельно проаналізувати джерела, нормативну базу, та саму матеріал по цій темі, а також створити комплексне уявлення про проблему інформаційної безпеки, виокремити основні аспекти та встановити взаємозв'язки між різними складовими цієї сфери, такими як сама інформаційна безпека, безпека інформації, та кібербезпека.

Історичний метод був використаний у дослідженні для вивчення історії розвитку системи забезпечення інформації безпеки в Україні. Цей метод дозволив відтворити тему дослідження у історичному аспекті. Які етапи становлення та розвитку системи інформаційної безпеки були проїдені в Україні. Які нормативні-правові акти були створені, втратили чинності, та які документи прийшли на їх заміну застарілим, чи ті закони що були створені ще в часи становлення держави, а до сих пір виконують свою задачу по регулюванню інформаційної безпеки. Завдяки методу історичного аналізу були обґрунтовані висновки щодо змін у цій сфері протягом всього часу.

Метод бібліографічної евристики був необхідним для ефективного пошуку та аналізу наукової літератури та статей, що стосується інформаційної безпеки в

Україні. Завдяки цьому методу була здійснена обширна робота із знаходження та оцінки джерел, що становлять основу дослідження.

Методом спостереження було зафіксовано як інформаційна безпека реалізується в Секретаріаті Кабінету Міністрів України, в рамках того доступу до інформації що мені було надано у сьогоднішній нелегкий час [додаток В].

За допомогою методу узагальнення були сформульовані конкретні висновки, які відображають інформаційний контекст та важливість обраної теми дослідження.

Отже, загальною метою використання цих методів було досягнення глибокого розуміння та побудови моєї кваліфікаційної роботи за темою організація захисту інформації в Секретаріаті Кабінету Міністрів України, а також розробка обґрунтованих висновків, які сприятимуть подальшому вдосконаленню та залученню інтересу до системи забезпечення безпеки інформації в країні.

Таким чином в першому розділі було проаналізовано низку наукових праць авторів та нормативно-правової бази які пов’язані з темою організації захисту інформації. Також були показанні методи наукового дослідження, які були використані в мої кваліфікаційній роботі.

РОЗДІЛ 2.
ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

2.1. Захист інформації в кіберпросторі

Інформаційна безпека та захист інформації є надзвичайно важливими для України. З моменту проголошення незалежності Україна стала об'єктом інформаційної агресії з боку зовнішніх акторів, які намагаються впливати на її внутрішні справи та сприяти нестабільності в країні. Інформаційна безпека має вирішальне значення для захисту національних інтересів і запобігання стабільності в Україні. Для цього важливо забезпечити захист інформації від несанкціонованого доступу, зловживання та витоку, а також використання інформаційних технологій у злочинній діяльності [51].

Крім того, інформаційна безпека є невід'ємною частиною національної безпеки, яка захищається засобами запобігання зовнішнім загрозам, включаючи тероризм, кіберзлочинність та інформаційну війну.

Україна зробила значний крок у напрямку забезпечення інформаційної безпеки шляхом прийняття закону «Про основні засади забезпечення кібербезпеки в Україні», цей закон регулює провадження діяльності у сфері інформаційної безпеки та визначає основні принципи діяльності в цій сфері. Також було створено державну службу кібербезпеки, яка відповідає за координацію діяльності в цій сфері. Однак, для досягнення повної інформаційної безпеки в Україні необхідно продовжувати працювати над розвитком відповідних законодавчих актів та підвищення рівня кібербезпеки в усіх сферах, включаючи державні органи, бізнес-структури та громадські організації [5].

Крім того, необхідно забезпечити широку доступність інформації про загрози у сфері кібербезпеки та профілактичні заходи, які можна вжити. Також існує потреба в розбудові потенціалу експертів у сфері кібербезпеки та залученні молоді до досліджень і розробок у цій галузі. Розвиток інформаційної безпеки в

Україні створить сприятливе середовище для розвитку інноваційних технологій та електронної комерції, що позитивно вплине на економіку України та забезпечить її міжнародну конкурентоспроможність. Забезпечення інформаційної безпеки є складним і багатогранним завданням, яке потребує спільних зусиль держави, підприємств і суспільства. Але, працюючи разом, Україна може створити безпечне та сприятливе середовище для розвитку своїх національних інтересів [47].

Етапи еволюції державного управління інформаційною безпекою в Україні [44]:

1-й етап (1991–1997 рр.) – у спадок від СРСР нашій державі дісталась класична бюрократична модель державного управління (модель адміністративно-державного управління), у світовій практиці вона відома під назвою «Old Public Management (Старе Державне Управління)» . До характерних особливостей цієї моделі належать перш за все:

а) ієрархічний, вертикально інтегрований спосіб організації системи управління, з чітким розмежуванням повноважень, субординацією для різних рівнів органів і посадових осіб;

б) прямий (адміністративний) державний контроль за всіма сферами життєдіяльності;

в) відокремленість і закритість влади від суспільства.

2-й етап (1998–2005 рр.) – початок нового етапу ознаменувався кардинальною зміною розуміння феномену «інформаційної безпеки». В прийнятому 4 лютого 1998 року Законі України «Про Концепцію Національної програми інформатизації» «інформаційна безпека», на відміну від першого етапу, вже характеризується, як невід’ємна частина політичної, економічної, оборонної та інших складових національної безпеки.

3-й етап (2006–2013 рр.) – характеризується кардинальними змінами у державному управлінні інформаційною безпекою, інтенсивною роботою з визначення концептуальних засад системи забезпечення інформаційної безпеки

в Україні. Розпочалась розробка засад, які б стали основою концепції для нової державної політики забезпечення інформаційної безпеки України. Вони мали базуватися на постулатах та цінностях громадянського суспільства, відповідати сучасним європейським нормам, упровадження яких розглядається як безпосередній обов'язок держави.

4-й етап (2014–2022 рр.) – в історичній динаміці становлення і розвитку системи забезпечення інформаційної безпеки України має особливий двоїстий характер оскільки, по-перше, виступаючи логічним продовженням еволюції державного управління інформаційною безпекою, характеризується вирішенням важливих стратегічних питань державної політики із забезпечення інформаційної безпеки в умовах інформаційно-психологічного протиборства, по-друге, виступає окремою, абсолютно новою віхою в історії державного управління забезпеченням інформаційної безпеки України.

5-й етап (2022 – до сьогодні) – сучасна російсько-українська війна стала новим викликом для системи забезпечення інформаційної безпеки України. Військова агресія Росії призвела до посилення інформаційно-пропагандистського протиборства, що вимагає від України нових підходів до захисту своїх інформаційних ресурсів.

На сучасному етапі розвитку системи забезпечення інформаційної безпеки України актуальними є такі завдання:

а) посилення інформаційно-пропагандистського протиборства з РФ;

б) захист українських інформаційних ресурсів від кібератак;

в) створення ефективної системи інформаційної безпеки для органів державної влади, бізнесу та суспільства;

г) підвищення рівня обізнаності населення про загрози інформаційної безпеки.

За останні роки Україна зробила значні кроки в розвитку кібербезпеки. Однак, кібербезпека є складною та багатогранною сферою, і постійно виникають нові виклики. Для забезпечення ефективного захисту інформації Україні

необхідно продовжувати впроваджувати нові технології та практики, а також підвищувати рівень обізнаності суспільства про кібербезпеку [48].

Кібербезпека – це галузь комп'ютерних наук, яка займається захистом комп'ютерних систем, мереж і програм від несанкціонованого доступу, використання, модифікації або знищення. Кіберзагрози – це будь-який акт, який може завдати шкоди комп'ютерній системі, мережі або програмі. Кіберзагрози можуть бути здійснені як окремими особами, так і організованими групами або державними структурами [48].

Кібератаки – це спроба незаконного звернення до комп'ютерних систем або мереж з метою злому, крадіжки, розповсюдження шкідливих програм або знищення даних. В Україні кібератаки можуть включати в себе такі види нападів, як DDoS-атака, фішинг, злам аккаунтів, викрадення даних, розповсюдження шкідливих програм, кібершпигунство та інші. Нападники можуть бути як окремими особами, так і організованими групами або державними структурами, які намагаються використовувати кібератаки для своїх власних цілей. Для захисту від кібератак в Україні створено Центр кібербезпеки при Державній службі спеціального зв'язку та захисту інформації, який відповідає за забезпечення кібербезпеки в країні [48].

Віруси та шкідливі програми є серйозними загрозами для інформаційної безпеки в Україні. Вони можуть пошкодити або викрасти конфіденційну інформацію, знищити дані, заблокувати комп'ютерну систему та вимагати викуп. Шкідливі програми також можуть використовуватися для злочинних цілей, таких як злочинність в інтернеті, шахрайство та ідентифікаційний крадіжки. Українські компанії та уряд повинні ретельно перевіряти вхідну та вихідну інформацію, встановлювати антивірусні програми та здійснювати регулярне оновлення програмного забезпечення. Також важливо навчати користувачів інтернету про безпечне користування комп'ютерами та іншими пристроями, а також про захист своїх персональних даних [48]. Ось кілька

прикладів вірусів та шкідливих програм, які були поширені в Україні в останні роки:

а) вруси-шпигуни, які можуть збирати інформацію про користувачів, таку як паролі, номери кредитних карток та особисті дані.

б) віруси-блокатори, які можуть заблокувати комп'ютерну систему і вимагати викуп за розблокування.

в) віруси-шифровщики, які можуть шифрувати дані на комп'ютері і вимагати викуп за розшифрування.

Спам-пошта – це надмірне надходження небажаних листівок або електронної пошти, які містять рекламу, маркетингові повідомлення або навіть шкідливі віруси. Вона може викликати перевантаження поштових серверів та витрачати час та ресурси користувача на фільтрацію та видалення небажаних повідомлень. Спам-пошта також може бути використана як інструмент фішингу, коли зловмисники намагаються отримати конфіденційну інформацію від користувача, переконуючи його надіслати свої дані через пошту [48]. Ось кілька прикладів спаму, який було поширено в Україні в останні роки:

а) спам, що містить рекламу товарів і послуг, які не цікавлять користувача.

б) спам, що містить шкідливі віруси.

в) спам, що містить фішингові повідомлення, які намагаються отримати конфіденційну інформацію від користувача.

Фішинг – це спосіб шахрайства, який полягає в тому, що зловмисники використовують електронну пошту, соціальні мережі, SMS-повідомлення та інші канали комунікації для того, щоб отримати доступ до їхніх конфіденційних даних, таких як паролі, номери банківських карток тощо [48].

Соціальний інженерінг – це техніка обману, яка полягає в використанні маніпуляцій та психологічних впливів з метою отримання конфіденційної інформації або здійснення інших злочинних дій. Цей вид шахрайства зазвичай залучає людей до виконання певних дій або надання доступу до інформації, які можуть бути шкідливими для них або їхніх організацій. Найпоширеніші методи

соціального інженерінгу – це відправлення фішингових електронних листів, використання соціальних мереж та підроблення ідентифікаційних даних [48].

DDoS-атаки (Розподілена відмова в обслуговуванні) – це техніка кібератак, при якій велика кількість запитів надсилається до вебсайту або комп'ютерної мережі з метою перевантаження їх ресурсів та зниження їх доступності для користувачів. У результаті цих атак, вебсайти та мережі можуть бути тимчасово або повністю недоступні, що може спричинити серйозні проблеми для бізнесу та інших організацій, які залежать від доступності своїх вебсайтів і мереж для роботи. Для здійснення DDoS-атак використовуються ботнети, що складаються з великої кількості комп'ютерів, які заздалегідь були заражені шкідливими програмами [48].

Несанкціонований доступ до конфіденційної інформації – це отримання несанкціонованою особою доступу до інформації, яка захищена законом від розголошення та не має бути доступною загальному колу користувачів. Це може статися шляхом використання шпигунського програмного забезпечення, вразливостей в програмному забезпеченні, соціальної інженерії, а також інших методів. Несанкціонований доступ до конфіденційної інформації може призвести до її викрадення, втрати, пошкодження, розголошення або використання відповідно до недобрих намірів.

Кібершантаж – це форма електронного шахрайства, яка полягає в тому, що зловмисники вимагають від потенційних жертв грошову винагороду або інші послуги, загрожуючи розкриттям їхньої конфіденційної інформації або завданням шкоди їхній репутації в інтернеті. Кібершантаж може відбуватися за допомогою різноманітних методів, таких як відправка підроблених електронних листів, вимагання відкриття шкідливого посилання, шифрування важливих даних або блокування доступу до важливих ресурсів. Кібершантаж є серйозною загрозою для бізнесу, оскільки він може призвести до втрати даних, фінансових втрат і репутаційних збитків [48].

Як захистити себе від кібершантажу:

а) бути пильним при відкриванні електронних листів. Не відкривати електронні листи від невідомих відправників, а також електронні листи, які містять посилання або вкладення, які ви не впевнені;

б) використовувати надійні антивірусні програми і брандмауери. Антивірусні програми і брандмауери допоможуть захистити комп'ютер від шкідливого програмного забезпечення, яке може використовуватися для кібершантажу.

в) регулярно оновлювати програмне забезпечення. Оновлення програмного забезпечення часто містять виправлення безпеки, які можуть допомогти захистити комп'ютер від кібератаків.

г) зробити резервну копію важливих даних. Якщо дані будуть викрадені в результаті кібератаки, резервна копія допоможе вам відновити їх.

д) не плати зловмисникам. У разі кібершантажу, не платити зловмисникам. Це лише погіршить ситуацію і може призвести до подальших кібератак.

е) повідомити про інцидент в поліцію. Поліція зможе допомогти розслідувати інцидент і затримати зловмисників.

Дезінформація – це поширення невірної або зміненої інформації з метою збитку або маніпулювання. Це може бути здійснено через соціальні мережі, електронну пошту, вебсайти та інші канали масової інформації. Розповсюдження дезінформації може мати серйозні наслідки, такі як:

а) погіршення відносин між державами;

б) розпалювання конфліктів;

в) зниження довіри до інформаційних джерел;

г) сприяння екстремізму та тероризму;

д) створення сприятливого середовища для маніпулювання людьми.

Деякі приклади дезінформації включають:

а) поширення неправдивих новин про події, наприклад, про вибори або військові конфлікти;

б) створення фейкових вебсайтів, які виглядають як реальні новинні сайти;

в) розсилання електронних листів, які містять шкідливе програмне забезпечення або посилання на фейкові вебсайти;

г) використання соціальних мереж для поширення неправдивої інформації про людей або організації;

Кібершпигунство – це процес отримання конфіденційної інформації, використовуючи комп'ютерні технології та інтернет. Кібершпигуни можуть використовувати шпигунське програмне забезпечення, соціальний інженерінг та інші техніки для злому комп'ютерних систем та мереж, а також для перехоплення передачі інформації. Одним з найбільш поширених видів кібершпигунства є викрадення ідентифікаторів доступу до різноманітних систем та ресурсів. Такі дії можуть бути спрямовані як на отримання комерційної користі, так і на здійснення політичних або кримінальних дій [48].

Деякі приклади кібершпигунства включають:

а) злом комп'ютерних систем урядових установ;

б) викрадання конфіденційної інформації з банківських систем;

в) розголошення конфіденційної інформації про компанії або організації;

г) шантажування людей або організацій;

д) створення кіберзброї, яка може бути використана для завдавання шкоди або загибелі людей.

Кіберзброя – це будь-який програмний або апаратний засіб, який використовується для завдавання шкоди комп'ютерним системам або мережам. Кіберзброя може бути використана для різних цілей, зокрема для крадіжки даних, саботажу інфраструктури та поширення дезінформації.

Існує багато різних типів кіберзброї, але деякі з найпоширеніших включають:

а) віруси – це шкідливе програмне забезпечення, яке може поширюватися з одного комп'ютера на інший без відома користувача. Віруси можуть завдавати

шкоди комп’ютерним системам різними способами, зокрема видаленням файлів, пошкодженням системних файлів або перехопленням керування комп’ютером;

б) троянські коні – це шкідливе програмне забезпечення, яке маскується під безневинну програму. Коли користувач запускає троянського коня, він інсталює шкідливе програмне забезпечення на комп’ютер. Троянські коні можуть використовуватися для крадіжки даних, саботажу інфраструктури або поширення інших шкідливих програм;

в) шпигунські програми – це шкідливе програмне забезпечення, яке збирає інформацію про користувача без його відома. Інформація, яка збирається шпигунськими програмами, може включати особисті дані, такі як паролі, кредитні картки та номери телефонів. Шпигунські програми можуть використовуватися для крадіжки особистих даних або для поширення дезінформації;

г) віруси-боти – це шкідливе програмне забезпечення, яке може контролювати комп’ютер зловмисника. Віруси-боти можуть використовуватися для створення мережі комп’ютерів, які називаються ботнетами. Ботнети можуть використовуватися для різних цілей, зокрема для поширення спаму, DDoS-атак і крадіжки даних.

Кіберзброя є серйозною загрозою для приватності, безпеки інфраструктури та економіки. Для захисту від кіберзброї важливо мати налаштовані заходи безпеки, зокрема антивірусне програмне забезпечення, брандмауер і регулярні оновлення програмного забезпечення [48].

Кібербезпека, кібергігієна та кіберзахист – це три основні види заходів, які використовуються для захисту комп’ютерних систем, мереж та даних від різних видів кібератак [57].

Кібербезпека – це комплексний підхід до захисту комп’ютерних систем, мереж та даних від широкого спектру небажаних атак, вірусів, вразливостей та інших загроз, що можуть завдати шкоди їхній цілісності, конфіденційності та доступності. Система заходів забезпечує захист від кіберзлочинців,

кібершпигунів та інших зловмисників, які можуть мати намір отримати несанкціонований доступ до конфіденційних даних, викрасти їх або завдати шкоди комп'ютерним системам і мережам [35].

Основні види заходів, які використовуються для забезпечення кібербезпеки, включають в себе:

а) регулярне оновлення програмного забезпечення;

б) встановлення антивірусних програм та файрволів;

в) використання складних паролів та методів аутентифікації;

г) використання криптографічних методів захисту даних;

д) резервне копіювання даних;

е) інші технічні та організаційні заходи.

Також важливим елементом кібербезпеки є освіта та підвищення свідомості користувачів щодо безпеки в інтернеті, а також регулярне проведення аудитів з метою виявлення вразливостей і підвищення рівня захисту.

Кібергігієна – це сукупність правил, рекомендацій та поведінкових навичок, які допомагають зберегти безпеку та конфіденційність в інтернеті. Основна мета кібергігієни полягає в тому, щоб захистити користувача від різних видів кібератак та кіберзлочинів. Основні принципи кібергігієни включають:

а) збереження паролів та інших конфіденційних даних у безпечному місці;

б) використання надійного антивірусного програмного забезпечення та регулярні оновлення його до новішої версії;

в) встановлення оновлень для операційної системи та програм, що використовуються на пристроях;

г) використання захищених каналів зв'язку для передачі конфіденційної інформації, такої як паролі, банківські дані тощо;

д) безпечне використання соціальних мереж та інших онлайн-платформ, включаючи збереження приватності та обмеження доступу до особистої інформації;

е) не відповідайте на електронні листи від невідомих або підозрілих відправників та не відкривайте посилання та вкладення, якщо ви не очікуєте їх;

ж) використання складних та унікальних паролів для кожного облікового запису та регулярна зміна їх.

Кіберзахист – це комплекс заходів, спрямованих на захист комп'ютерних систем, мереж та даних від різних видів кібератак та інших небезпек, пов'язаних з використанням інформаційних технологій. Кіберзахист передбачає використання технічних, організаційних та правових засобів, таких як встановлення брандмауерів, антивірусного програмного забезпечення, моніторинг мережі, резервне копіювання даних, планування дій у разі кібератаки та багато іншого.

Всі три аспекти кібербезпеки (кібербезпека, кібергігієна та кіберзахист) важливі для забезпечення безпеки комп'ютерних систем, мереж та даних. Важливо розуміти, що кібератаки постійно розвиваються, тому важливо постійно оновлювати свої знання та навички в галузі кібербезпеки, щоб захистити себе від сучасних загроз.

Крім технічних засобів, кіберзахист також включає навчання користувачів правилам безпечного користування комп'ютерами та іншими пристроями, а також захисту персональних даних та конфіденційної інформації в інтернеті. Кіберзахист є важливим елементом захисту національної кібербезпеки, оскільки забезпечує захист не лише окремих користувачів та компаній, але й державних структур від можливих кібератак, які можуть завдати значних збитків економіці та інфраструктурі країни.

Якщо аналізувати самі тенденції забезпечення інформаційної безпеки то в нас з'являться такі результати. Кібербезпека – це стан захищеності інформаційних систем та мереж від несанкціонованого доступу, використання, розголошення, модифікації або знищення інформації. Кібербезпека є важливим аспектом безпеки будь-якої організації, яка використовує комп'ютери та мережі

Система кібербезпеки повинна включати в себе як технічні, так і організаційні заходи [5].

Технічні заходи кібербезпеки включають у себе використання антивірусного програмного забезпечення, брандмауерів, фільтрів контенту та інших технологій, які допомагають захистити інформаційні системи та мережі від несанкціонованого доступу.

Організаційні заходи кібербезпеки включають у себе навчання співробітників правилам кібербезпеки, розробку процедур реагування на кібератаки та створення системи управління кібербезпекою.

Ефективність системи кібербезпеки залежить від багатьох факторів, зокрема від складності системи, рівня загроз, а також від досвіду та кваліфікації персоналу, який відповідає за кібербезпеку. Перспективи розвитку системи кібербезпеки пов’язані з розробкою нових технологій захисту інформації, а також з підвищенням рівня обізнаності співробітників про кіберзагрози [50].

Організаційна система забезпечення інформаційної безпеки держави визначає такі рівні:

І рівень – стратегічний, загальнодержавний, який включає ВРУ, Президента України, КМУ, та полягає у прийнятті політичних рішень, законодавчого і нормативно-правового забезпечення, встановлення порядку міжнародного співробітництва та ін.

ІІ рівень – організаційно-виконавчий, відомчо-територіальний, який включає центральні органи виконавчої влади, органи місцевого самоврядування, правоохоронні органи та органи судової влади. На вказаному рівні здійснюється організаційне і методичне забезпечення інформаційної безпеки у відповідних галузях та адміністративно-правових утвореннях, координація і контроль діяльності у сферах відповідальності державно-владних структур.

ІІІ рівень – критично важливі інфраструктури країни, до яких доцільне включення підприємств, установ, організацій, комунікацій національного інформаційного простору та інших об’єктів, управління якими здійснюється з

використанням електронно-комунікаційних засобів та інформаційних технологій.

IV рівень – рівень суб'єктів невладного характеру, до яких відносяться громадяни України, їх об'єднання, державні і приватні засоби масової інформації [32].

Таблиця 1 – Періодизація розвитку державного управління забезпеченням інформаційної безпеки [23, с. 3–4]

№ з/п	Період	Характеристика
1	1991-1997 рр.	формування сукупності інститутів державної влади, що забезпечуватимуть прямий державний контроль та різновекторний вплив на інформаційний простір України
2	1998-2005 рр.	формування нормативно-правових основ і структури управління інформаційною безпекою та визначення її як окремого об'єкта державної політики. Поняття «інформаційна безпека» набуло нового вигляду, що вже почало ототожнюватися, як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки
3	2006-2013 рр.	кардинальними змінами у державному управлінні інформаційною безпекою, інтенсивною роботою з визначення концептуальних засад системи забезпечення інформаційної безпеки в Україні. Розпочалась розробка засад, які б стали основою концепції для нової державної політики забезпечення інформаційної безпеки України.

4	З 2014 р. – по теперішній час	кардинальні трансформаційні зміни у відносинах між державою і громадянським суспільством, починають запроваджуватись нові способи і механізми державного управління, що спроможні забезпечити ефективне управління суспільними процесами в сучасних умовах

Технічні заходи кібербезпеки є одним із найважливіших компонентів системи кібербезпеки. Технічні заходи допомагають захистити інформаційні системи та мережі від несанкціонованого доступу, використання, розголошення, модифікації або знищення інформації.

До технічних заходів кібербезпеки належать:

а) антивірусне програмне забезпечення;

б) брандмауери;

в) фільтри контенту;

г) системи виявлення та запобігання вторгненням (IDS/IPS);

д) системи управління доступом (IAM);

е) системи шифрування;

ж) системи резервного копіювання;

и) організаційні заходи кібербезпеки.

Організаційні заходи кібербезпеки є не менш важливими, ніж технічні заходи. Організаційні заходи допомагають підвищити обізнаність співробітників про кіберзагрози, а також розробити процедури реагування на кібератаки.

До організаційних заходів кібербезпеки належать:

а) навчання співробітників правилам кібербезпеки;

б) розробка процедур реагування на кібератаки;

в) створення системи управління кібербезпекою;

г) ефективність системи кібербезпеки.

Ефективність системи кібербезпеки залежить від багатьох факторів, зокрема від складності системи, рівня загроз, а також від досвіду та кваліфікації персоналу, який відповідає за кібербезпеку. Комплексний підхід до кібербезпеки, який включає в себе як технічні, так і організаційні заходи, є найбільш ефективним способом захисту інформаційних систем та мереж від кібератак.

Перспективи розвитку кібербезпеки пов’язані з розробкою нових технологій захисту інформації, а також з підвищенням рівня обізнаності співробітників про кіберзагрози. Розвиток нових технологій захисту інформації дозволяє створювати більш ефективні системи кібербезпеки. Наприклад, використання технології штучного інтелекту дозволяє виявляти кібератаки на ранніх стадіях. Підвищення рівня обізнаності співробітників про кіберзагрози також є важливим фактором підвищення ефективності системи кібербезпеки. Співробітники повинні бути обізнані про кіберзагрози, такі як фішинг, кібершахрайство та інші, а також про правила кібербезпеки, які допоможуть захистити їхню організацію від кібератак [71].

Отже, мою було доведено що сучасна інформаційна безпека має під собою великий досвід, але за тенденціями сучасного часу, зараз більше за все люди акцентують увагу кібербезпеці з усіма новими технологіями. Вона є одним із важливих напрямів захисту інформації як на рівні державного управління, так і на рівнях структур різного підпорядкування та стосується безпосередньо кожним громадянином України.

2.2. Партнерство з приватним сектором та міжнародними партнерами для підвищення ефективності захисту інформації у сфері державного управління

Партнерство між державним та приватним сектором, а також міжнародними партнерами є важливим кроком у підвищенні ефективності захисту інформації в Україні. Забезпечення безпеки інформації є надзвичайно важливим завданням в умовах сучасного цифрового світу, де загрози кібербезпеці постійно зростають.

Державний сектор має великий потенціал та відповідальність у забезпеченні захисту інформації. Для досягнення максимальної ефективності, важливо побудувати партнерські відносини з приватним сектором, який має необхідні знання та ресурси для впровадження сучасних технологій та заходів з кібербезпеки [34].

Також важливо співпрацювати з міжнародними партнерами, які можуть надати підтримку в розробці стратегій та впровадженні передових методів захисту інформації. Міжнародний обмін досвідом та експертизою допоможе підвищити рівень кібербезпеки в Україні та спрямувати зусилля на досягнення найвищих стандартів захисту інформації.

Україна вже має певний досвід у побудові такого партнерства. Наприклад, створення Національного центру кібербезпеки України (НЦКБ) є важливим кроком у координації зусиль державного та приватного сектору у сфері кібербезпеки. Додаткові проєкти та ініціативи, спрямовані на співпрацю та обмін інформацією, допоможуть підвищити ефективність захисту інформації у всіх сферах діяльності.

Залучення приватного сектору до процесу захисту інформації дозволить використовувати інноваційні рішення та передові технології, що покращать реагування на кіберзагрози та запобігання інцидентам. Водночас, співпраця з міжнародними партнерами надасть доступ до світових стандартів та кращих

практик в галузі кібербезпеки. Важливо встановити механізми обміну інформацією та взаємодії між всіма сторонами партнерства.

Регулярні зустрічі, форуми, тренінги та семінари допоможуть сприяти обміну досвідом, підвищити обізнаність про загрози та зміцнити спільну працездатність. Партнерство між державним та приватним сектором, а також міжнародними партнерами, сприятиме підвищенню ефективності захисту інформації в Україні. Тільки через спільні зусилля та взаємодію можна досягти стійкого кібербезпекового середовища, яке буде забезпечувати захист інформації та сприяти розвитку країни у цифрову епоху.

Досвід свідчить, що партнерство між державним та приватним сектором та міжнародне партнерство дозволяють підвищити рівень кібербезпеки в Україні шляхом взаємовигідної співпраці у таких напрямах:

а) державний сектор може надати фінансування для розробки та впровадження кібербезпекових технологій та рішень;

б) приватний сектор може надати експертні консультації та допомогу в розробці та впровадженні кібербезпекових стратегій;

в) міжнародні партнери можуть надати доступ до світових стандартів та кращих практик в галузі кібербезпеки.

Партнерство між державним та приватним сектором, а також міжнародними партнерами, є ключовим фактором підвищення рівня кібербезпеки в Україні. Тільки через спільні зусилля та взаємодію можна досягти стійкого кібербезпекового середовища, яке буде забезпечувати захист інформації та сприяти розвитку країни у цифрову епоху.

Україна має кілька державних установ та органів, які займаються питаннями інформаційної безпеки. Зокрема, Міністерство цифрової трансформації України (МЦТ), яке було створене в 2019 році з метою прискорення цифрової трансформації країни та досягнення європейського рівня розвитку в галузі цифрових технологій. Головне завдання Міністерства – забезпечення розвитку та впровадження цифрових технологій у всіх галузях

життя, а також покращення якості державних послуг і підвищення рівня цифрової грамотності населення [65].

Основні завдання Міністерства цифрової трансформації України включають розробку та впровадження стратегії цифрової трансформації України; забезпечення розвитку та впровадження цифрових технологій у всіх галузях життя, включаючи промисловість, освіту, медицину, транспорт тощо; запровадження електронних державних послуг та створення інфраструктури для їх надання; захист інформаційної безпеки держави, включаючи захист від кібератак та інших кіберзагроз; підвищення рівня цифрової грамотності населення та підготовка кадрів в галузі інформаційних технологій.

Національного центру кібербезпеки України (НЦКБ) – це державна установа в Україні, створена з метою забезпечення національної кібербезпеки та протидії кіберзагрозам. Основними завданнями центру є:

а) моніторинг, виявлення та аналіз кіберзагроз, забезпечення оперативного реагування на них;

б) розробка та реалізація стратегії державної політики з питань кібербезпеки; координація дій установ та організацій, які забезпечують кібербезпеку в Україні;

в) забезпечення взаємодії з партнерами в галузі кібербезпеки на національному та міжнародному рівнях;

г) проведення науково-технічних досліджень та розробок у галузі кібербезпеки [15].

НЦКБ був головною структурою до 2016 року, на його зміну була створена державна служба спеціального зв’язку та захисту інформації України.

Державна служба спеціального зв’язку та захисту інформації України (ДССЗІ) – це державний орган спеціального призначення, який відповідає за захист інформації в Україні, зокрема, за захист від кібератак, кібершпигунства, кібертероризму та інших загроз. ДССЗІ є головним органом у сфері захисту інформації в Україні. ДССЗІ співпрацює з іншими державними органами,

приватними компаніями та міжнародними організаціями з метою підвищення рівня кібербезпеки в Україні. ДССЗІ створено в 2016 році на базі Національного центру кібербезпеки України. Основні завдання ДССЗІ полягають у забезпеченні державної політики в сфері захисту інформації; захисті державних та публічних інформаційних ресурсів від кібератак та інших кіберзагроз; захисті персональних даних громадян України; Розслідуванні кібератак та інших кіберзлочинів; просвітницькій роботі з питань кібербезпеки [6].

Служба безпеки України (СБУ) – це державний орган спеціального призначення, який відповідає за забезпечення національної безпеки України, у тому числі за захист від кіберзагроз та кібертероризму. Основні завданням СБУ полягають у забезпеченні національної безпеки України та її суверенітету; захисті конституційних прав і свобод людини та громадянина; захисті України від зовнішніх і внутрішніх загроз; протидії кіберзагрозам та кібертероризму; забезпеченні безпеки громадян України за кордоном [14].

Національна поліція України (далі – НПУ) – це основний орган виконавчої влади, який забезпечує правопорядок та безпеку громадян в Україні. Цілі та завдання Національної поліції України включають забезпечення законності та правопорядку в країні шляхом запобігання злочинам, розкриття злочинів, затримання та притягнення до відповідальності правопорушників; захист прав та свобод людини та громадянина, що передбачає захист громадського порядку, безпеки держави та її громадян; забезпечення безпеки в інтернеті та боротьба з кіберзлочинністю, зокрема виявлення та розслідування кіберзлочинів, запобігання кібератакам та іншим інформаційним загрозам; проведення профілактичної та виховної роботи з населенням з питань кібербезпеки та кіберзахисту; співпраця з іншими національними та міжнародними організаціями з питань кібербезпеки та обмін досвідом [13].

Особлива увага приділяється боротьбі з кіберзлочинністю, оскільки це стає все більш актуальною проблемою в сучасному цифровому світі. НПУ бере активну участь у протидії кіберзагрозам та здійснює необхідні заходи для

забезпечення кібербезпеки в Україні. Всі ці органи співпрацюють задля забезпечення України від кіберзагроз.

Приватний сектор інформаційної безпеки в Україні може включати різні компанії з кібербезпеки, зокрема, приватні компанії, що спеціалізуються на наданні послуг з кібербезпеки, зокрема:

а) аудит безпеки – це процес оцінки стану безпеки інформаційних систем та мереж. Аудит безпеки може виявити слабкі місця в системах безпеки, які можуть бути використані зловмисниками для атаки;

б) виявлення інцидентів, що дозволяє виявляти та реагувати на інциденти кібербезпеки. Інцидент кібербезпеки – це будь-яка подія, яка може порушити безпеку інформаційних систем або мереж;

в3) впровадження заходів безпеки – це процес впровадження заходів, які допомагають захистити інформаційні системи та мережі від атак. Заходи безпеки можуть включати використання антивірусного програмного забезпечення, брандмауерів, систем виявлення вторгнень та інших технологій;

г) розробка програмного забезпечення для захисту інформації, яке допомагає захистити інформацію від несанкціонованого доступу, використання або розкриття. Програмне забезпечення для захисту інформації може включати антивірусне програмне забезпечення, брандмауери, системи виявлення вторгнень та інші технології.

Важливим є співпраця з постачальниками послуг хмарного зберігання. Хмарні сервіси – це послуги зберігання даних, обробки та передачі інформації в інтернеті. Хмарні сервіси можуть надаватися різними компаніями, зокрема: гугл, вебсервіс амазон та майкрасофт азур. До них висуваються вимоги щодо високого рівня захисту інформації, зокрема шифрування даних та механізми контролю доступу.

Компанії, які розробляють програмне забезпечення, повинні враховувати аспекти кібербезпеки під час процесу розробки та забезпечити, щоб їхні продукти були захищені від потенційних загроз. Програмне забезпечення – це

будь-яка програма, яка може виконуватися на комп’ютері. Програмне забезпечення може бути використане для різних цілей, зокрема, для обробки інформації, управління системами та створення інтерфейсів користувача.

Компанії, що надають послуги у сфері IT, повинні мати внутрішні процедури та заходи безпеки, щоб захистити свою власну інформацію та інформацію клієнтів. IT-компанії можуть надавати різні послуги, зокрема підтримку комп’ютерів, мереж і програмного забезпечення.

Банки та інші фінансові установи також можуть бути залучені до організації системи кібербезпеки. Вони мають значний обсяг конфіденційної інформації про клієнтів, що обумовлює необхідність систем захисту для запобігання шахрайству, крадіжкам даних та іншим кіберзлочинам.

До компаній з електронної комерції онлайн-магазинів та платіжні системи висуваються вимоги щодо безпеки платежів, захисту персональних даних клієнтів та боротьби зі шахраями. Компанії з електронної комерції повинні використовувати різні заходи безпеки, зокрема шифрування даних, брандмауери та системи виявлення вторгнень.

У сфері критичної інфраструктури (енергетика, транспорт, зв’язок) мають мати високий рівень кібербезпеки для запобігання потенційним атакам, які можуть призвести до серйозних наслідків. Це пов’язано з тим, що критична інфраструктура – це системи та мережі, які є життєво важливими для функціонування суспільства. Критична інфраструктура може бути атакована зловмисниками для отримання доступу до конфіденційної інформації, порушення роботи систем або завдавання шкоди. Важливо, щоб приватний сектор інформаційної безпеки в Україні мав високий рівень експертизи, знань і технологій для ефективного захисту інформації та боротьби з кіберзагрозами.

Міжнародні організації є важливими партнерами для України в галузі кібербезпеки. Співробітництво з такими організаціями надає можливості для обміну інформацією, навчання та спільних дій з метою підвищення рівня захисту інформації. До таких міжнародних організацій, з якими Україна співпрацює в

галузі кібербезпеки є, зокрема, ЄС, з якою Україна має можливість співпрацювати в рамках європейської кібербезпекової архітектури. Це включає обмін інформацією, участь в спільних проєктах та ініціативах, а також підтримку в розробці національних стратегій та політик з кібербезпеки. Партнером України в галузі кібербезпеки є НАТО. Співробітництво з НАТО дозволяє Україні отримувати доступ до спеціалізованої експертизи та навчальних програм з кібербезпеки. Також проводяться спільні тренування та вправи для підвищення готовності до кібератак. З метою обміну інформацією, розробки спільних стандартів та проведення тренувань Україна співпрацює з ОБСЄ. Це сприяє зміцненню кібербезпекових здатностей України та підвищенню свідомості про кібербезпеку. Співпраця України з Інтерполом у сфері кібербезпеки доволяє ефективно вести боротьбу з кіберзлочинністю та обмінюватися інформацією про кіберзагрози шляхом спільних розслідувань, обміну даними та підтримки в розробці методів протидії кіберзлочинності [4].

Міжнародна співпраця включає різні джерела підтримки, зокрема, фінансову допомогу від урядів інших країн, міжнародних організацій та приватних фондів, що може бути використана для фінансування кібербезпекових ініціатив, таких як: розробка та впровадження національних стратегій кібербезпеки; оцінка ризиків. Так, оцінка кібербезпекових ризиків включає в себе аналіз потенційних загроз, уразливостей і наслідків кібератак. Важливим є розробка стратегії. На основі оцінки ризиків розробляється національна стратегія кібербезпеки. Стратегія містить конкретні цілі, завдання та заходи, які будуть впроваджені для зниження кібербезпекових ризиків. Впровадження стратегії включає в себе створення кібербезпекової інфраструктури, навчання персоналу і підвищення обізнаності про кібербезпеку. Важливим є регулярна оцінка виконання національної стратегії кібербезпеки. Це допоможе визначити, чи досягаються поставлені цілі, і в разі потреби внести корективи в стратегію.

Одним з напрямів організації захисту інформації є навчання та підготовка фахівців з кібербезпеки:, а саме: створення навчальних програм з кібербезпеки

для студентів і співробітників державних і приватних організацій; надання грантів для досліджень у галузі кібербезпеки; підтримка розробки нових технологій і інструментів кібербезпеки; проведення кібербезпекових кампаній на підвищення обізнаності серед населення.

Створення та модернізація ефективної кібербезпекової інфраструктури включає відкриття центрів кібербезпеки для захисту критичної інфраструктури; розробку і впровадження кібербезпекових заходів для захисту критичної інфраструктури; навчання та підготовку персоналу з кібербезпеки для захисту критичної інфраструктури.

Розслідування кібератак є невід'ємною складовою організації захисту інформації та інформаційної безпеки загалом. Цей напрям включає: оплату праці детективів, які проводять розслідування; оплату витрат на обладнання, яке використовується в розслідуванні, наприклад, ком'ютери, програмне забезпечення та обладнання для аналізу даних; оплату витрат на експертизу, наприклад, експертизу комп'ютерних систем і мереж; оплату витрат на навчання співробітників, які відповідають за кібербезпеку.

Розробка нових технологій для захисту від кібератак суттєво підвищує захист інформації. Важливим є про підвищення обізнаності про кібербезпеку серед громадськості, розробка плану реагування на кібератаки. Боротьба з кіберзлочинністю – одне зі складних завдань, яке стоїть перед відповідними органами. Вона включає розробку та впровадження кібербезпекових стандартів і практик; навчання та підвищення кваліфікації фахівців з кібербезпеки; розслідування кіберзлочинів і притягнення кіберзлочинців до відповідальності; розробку і впровадження кібербезпекових технологій; підтримку кібербезпекових досліджень і розробок.

Технічна допомога реалізується через надання необхідного обладнання, програмного забезпечення та послуг, потрібних для захисту інформаційних систем та мереж, зокрема, брандмауерів, антивірусних програм та систем виявлення вторгнень; надання систем управління ідентичністю та доступом,

систем управління конфіденційністю та систем управління інформаційною безпекою; надання послуг з навчання з кібербезпеки: консультування з кібербезпеки та реагування на інциденти в кіберпросторі.

Важливою у системі захисту інформації є консультативна підтримка, яка може бути надана у вигляді експертної поради та рекомендацій щодо розробки та впровадження кібербезпекових програм. Йдеться про надання порад щодо розробки національної стратегії кібербезпеки; рекомендацій щодо вибору та впровадження засобів кібербезпеки; допомоги в розробці та впровадженні програм навчання та підвищення кваліфікації з кібербезпеки.

Міжнародне партнерство в галузі інформаційної безпеки є важливим фактором для забезпечення ефективного захисту інформації в Україні та боротьби з кіберзагрозами. Співпраця з іншими країнами дозволяє обмінюватися досвідом, ресурсами та інформацією для створення стійкого кібербезпекового середовища.

Отже, партнерство у сфері інформаційної безпеки України є важливим чинником захисту кіберпростору від втручання в інформаційне середовище. Співпраця між органами влади, приватними компаніями, міжнародними організаціями, дає змогу зменшити напругу в цій сфері.

Таким чином, у цьому розділі була піднята загальну тему забезпечення інформаційної безпеки. Звісно за сучасними тенденціями зараз багато уваги приділяється технологічним аспектам, та як вони інтегрувалися в вже існуючу інформаційну безпеку. Було показано що співпраця між міністерствами, які під час своєї праці виконують постанови створюють кофенденційну інформацію, яка потребує забезпечення безпеки, приватними організаціями по забезпечувані інформаційної безпеки як для громадського населення чи державними контрактами. Також була проаналізована співпраця з міжнародними організаціями по обміну знаннями в сфері інформаційної безпеки.

РОЗДІЛ 3.
ВИМОГИ ДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В СЕКРЕТАРІАТІ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ

3.1. Структура Секретаріату Кабінету Міністрів України.

З метою вивчення структури Секретаріату Кабінету Міністрів (далі – СКМУ) України аналізувались відповідні законні і підзаконні акти. Зокрема, постанови КМУ «Про затвердження Регламенту Кабінету міністрів України» [21] Положення КМУ «Про затвердження Положення про Секретаріат Кабінету Міністрів України» [18], постанову КМУ «Про затвердження структури Секретаріату Кабінету Міністрів України» (остання редакція від 16 березня 2022 року) [19]. Це пов’язано з тим, що внаслідок російської агресії проти України та до цього періоду, було здійснено низку реформ, які призвели до реорганізації деяких міністерств через їх ліквідацію або об’єднання. Водночас значна інформація стала конфіденційною або секретною, тому у кваліфікаційній роботі використано лише ті дані, які є у публічній сфері.

Керівництво СКМУ складається з Міністра Кабінету Міністрів України та його заступників. Міністр Кабінету Міністрів України є головою Секретаріату і безпосередньо організовує його роботу. Він також подає для затвердження Кабінету Міністрів України пропозиції щодо структури Секретаріату та призначає на посаду і звільняє з посади працівників Секретаріату (крім керівника Апарату Прем’єр-міністра України).

До функцій Міністра Кабінету Міністрів України входить:

а) організація роботу Секретаріату;

б) подання для затвердження КМУ пропозицій щодо структури Секретаріату;

в) призначати на посаду і звільняти з посади працівників Секретаріату (крім керівника Апарату Прем’єр-міністра України);

г) затверджувати положення про структурні підрозділи;

д) контролювати виконання планів роботи КМУ;

е) подававати для схвалення Прем'єр-міністрові України проєкт порядку денного засідання КМУ;

ж) подавати Прем'єр-міністрові України на підпис прийняті Кабінетом Міністрів України (далі – КМУ) акти та схвалені проєкти для візування законів та актів Президента України;

и) проводити у разі потреби наради з керівниками центральних органів виконавчої влади для обговорення стану підготовки питань до розгляду на засіданнях КМУ урядових комітетів;

к) запитувати у міністерств, інших центральних і місцевих органів виконавчої влади, Ради міністрів Автономної Республіки Крим, підприємств, установ і організацій матеріали та інформацію з питань, що розглядаються КМУ та урядовими комітетами;

л) видавати з питань, що належать до його компетенції, накази та давати відповідні доручення працівникам Секретаріату.

Апарат Прем'єр-міністра України є допоміжним органом, який забезпечує здійснення Прем'єр-міністром України своїх повноважень. Апарат складається з керівника апарату, його заступників, а також інших працівників. Основними завданнями Апарату є:

а) моніторинг та аналіз ефективності реалізації КМУ політики в економічній, соціальній та інших сферах;

б) підготовка проєктів нормативно-правових актів з питань, що вносяться Прем'єр-міністром України на розгляд КМУ;

в) здійснення експертизи проєктів документів, що подаються на підпис Прем'єр-міністрові України;

г) забезпечення підготовки матеріалів для Прем'єр-міністра України до засідань КМУ, нарад, зустрічей;

д) здійснення інформаційного забезпечення діяльності Прем’єр-міністра України;

е) формування та підтримання політичного іміджу Прем’єр-міністра України;

ж) протокольне забезпечення офіційних заходів за участю Прем’єр-міністра України;

и) забезпечення та координація підготовки поточних і довгострокових робочих планів Прем’єр-міністра України, проведення нарад і зустрічей, здійснення закордонних візитів та поїздок по країні [18].

Апарат має право одержувати в установленому порядку від Секретаріату КМУ, служб віце-прем’єр-міністрів, центральних і місцевих органів виконавчої влади документи та інформацію, необхідні для виконання покладених на нього завдань. Апарат у своїй діяльності взаємодіє із структурними підрозділами СКМУ, Секретаріату Президента України та Апарату Верховної Ради України, центральних і місцевих органів виконавчої влади.

Служба Першого віцепре’єр-міністра України, віцепрем’єр-міністра України, Міністра Кабінету Міністрів України є допоміжним органом, який забезпечує діяльність цих посадових осіб. Служба складається з керівника служби, його заступників, а також інших працівників. Служба виконує широкий спектр завдань, зокрема сприяння реалізації політичних цілей Першого віцепрем’єр-міністра, створення належних умов для його роботи, забезпечення зв’язку з органами державної влади, органами місцевого самоврядування, громадськістю, іноземними та міжнародними організаціями, засобами масової інформації. Основними завданнями служби є:

а) сприяння реалізації політичних цілей Першого віцепрем’єр-міністра, віцепрем’єр-міністра;

б) створення належних умов для його роботи;

в) забезпечення зв’язку з органами державної влади, органами місцевого самоврядування, громадськістю, іноземними та міжнародними організаціями, засобами масової інформації.

Для виконання цих завдань служба виконує такі функції:

а) надає консультації з політичних та фахових питань;

б) забезпечує організацію робочого часу, опрацьовує робочі плани, організовує та забезпечує проведення нарад, зустрічей та поїздок;

в) здійснює попередній розгляд і аналіз документів;

г) готує доручення, здійснює контроль за їх виконанням;

д) приймає на підпис і візування документи;

е) організовує підготовку незалежних експертних висновків;

ж) узгоджує черговість та готує погодинні графіки розгляду питань на засіданнях урядових комітетів;

и) організовує підготовку матеріалів та готує тексти для виступів;

к) організовує прийоми делегацій і окремих відвідувачів;

л) координує діяльність радників.

Урядовий уповноважений з питань регуляторної політики – це посадова особа, уповноважена КМУ на виконання експертно-аналітичних та консультативно-дорадчих функцій з питань регуляторної політики.

Апарат Урядового уповноваженого з питань регуляторної політики є структурним підрозділом СКМУ. Він складається з керівника апарату, його заступників, а також інших працівників.

Урядовий уповноважений відповідно до покладених на нього завдань:

а) готує та подає КМУ пропозиції щодо координації роботи центральних і місцевих органів виконавчої влади з питань реалізації державної регуляторної політики;

б) вживає заходів стосовно захисту прав та законних інтересів суб’єктів господарювання внаслідок дії регуляторних актів;

в) інших питань, що належать до його компетенції;

г) бере участь у підготовці та опрацюванні структурними підрозділами СКМУ проєктів регуляторних актів та готує експертні висновки щодо регуляторного впливу таких актів;

д) вивчає факти та обставини, що спричинили порушення прав та законних інтересів суб'єктів господарювання внаслідок дії регуляторних актів;

е) бере за дорученням прем'єр-міністра України участь у засіданнях комітетів, тимчасових спеціальних та тимчасових слідчих комісій Верховної Ради України з питань, що стосуються його повноважень;

ж) взаємодіє з центральними і місцевими органами виконавчої влади, іншими державними органами, тимчасовими консультативними, дорадчими та іншими органами, що утворені КМУ, а також з органами місцевого самоврядування з питань, що належать до його компетенції.

Урядовий уповноважений з прав осіб з інвалідністю є посадовою особою, яка забезпечує здійснення КМУ своїх повноважень з питань захисту прав і законних інтересів осіб з інвалідністю та виконання Україною міжнародних зобов'язань у відповідній сфері. Основними завданнями Урядового уповноваженого є:

а) сприяння виконанню Україною міжнародних зобов'язань щодо додержання в Україні прав і законних інтересів осіб з інвалідністю;

б) моніторинг додержання прав і законних інтересів осіб з інвалідністю та підготовка в установленому порядку пропозицій щодо забезпечення додержання прав і законних інтересів осіб з інвалідністю;

в) вжиття у межах своїх повноважень заходів щодо усунення порушень прав і законних інтересів осіб з інвалідності та причин, що призвели до їх виникнення;

г) сприяння забезпеченню інформування громадськості про права осіб з інвалідністю.

Апарат Урядового уповноваженого з прав осіб з інвалідності є структурним підрозділом СКМУ, який забезпечує діяльність Урядового

уповноваженого. Апарат складається з керівника апарату, його заступників, а також інших працівників. Основними завданнями апарату є:

а) забезпечення організаційно-технічного та інформаційного забезпечення діяльності Урядового уповноваженого;

б) підготовка матеріалів для Урядового уповноваженого, зокрема проєктів звернень, заяв, рекомендацій, пропозицій, звітів;

в) координація діяльності представників Урядового уповноваженого у держадміністраціях вищого рівня;

г) співпраця з органами державної влади, органами місцевого самоврядування, громадськістю, міжнародними організаціями з питань захисту прав осіб з інвалідністю.

Урядовий уповноважений з питань гендерної політики є посадовою особою КМУ, яка забезпечує реалізацію державної політики у сфері забезпечення рівних прав та можливостей жінок і чоловіків у всіх сферах життя суспільства. Урядовий уповноважений має широкий спектр завдань, зокрема:

а) сприяння ефективній реалізації державної політики у сфері гендерної рівності;

б) координація дій з впровадження рекомендацій міжнародних інституцій з прав людини;

в) участь у розробці державних програм з питань гендерної рівності;

г) моніторинг та контроль за виконанням Національного плану з виконання резолюції Ради безпеки ООН;

д) співпраця з відповідними органами іноземних держав і міжнародних організацій;

е) інформування громадськості про гендерну рівність.

Апарат Урядового уповноваженого з питань гендерної політики є структурним підрозділом СКМУ, який забезпечує діяльність Урядового уповноваженого. Апарат складається з керівника апарату, його заступників, а також інших працівників. Основними завданнями апарату є:

а) забезпечення організаційно-технічного та інформаційного забезпечення діяльності Урядового уповноваженого;

б) підготовка матеріалів для Урядового уповноваженого;

в) координація діяльності представників Урядового уповноваженого у держадміністраціях вищого рівня;

г) співпраця з органами державної влади, органами місцевого самоврядування, громадськістю, міжнародними організаціями з питань гендерної рівності.

Урядовий уповноважений з питань гендерної політики є посадовою особою КМУ, яка забезпечує реалізацію державної політики у сфері забезпечення рівних прав та можливостей жінок і чоловіків у всіх сферах життя суспільства. Урядовий уповноважений має широкий спектр завдань, зокрема, сприяє:

а) ефективній реалізації державної політики у сфері гендерної рівності;

б) координації дій з впровадження рекомендацій міжнародних інституцій з прав людини;

в) розробці державних програм з питань гендерної рівності;

г) моніторингу та контроль за виконанням Національного плану з виконання резолюції Ради безпеки ООН;

д) співпраці з відповідними органами іноземних держав і міжнародних організацій;

е) інформуванню громадськість про гендерну рівність.

Апарат Урядового уповноваженого з питань гендерної політики є структурним підрозділом СКМУ, який забезпечує діяльність Урядового уповноваженого. Апарат складається з керівника апарату, його заступників, а також інших працівників. Основними завданнями апарату є:

а) забезпечення організаційно-технічного та інформаційного забезпечення діяльності Урядового уповноваженого;

б) підготовка матеріалів для Урядового уповноваженого;

в) координація діяльності представників Урядового уповноваженого у держадміністраціях вищого рівня;

г) співпраця з органами державної влади, органами місцевого самоврядування, громадськістю, міжнародними організаціями з питань гендерної рівності.

Директорат координації державних політик та стратегічного планування (Відділ СКМУ) є структурним підрозділом Секретаріату Кабінету Міністрів України, який відповідає за координацію реалізації державної політики, планування та моніторинг виконання стратегічних цілей та пріоритетів КМУ. Основними завданнями Директорату є:

а) координація діяльності органів виконавчої влади щодо реалізації державної політики;

б) розробка та впровадження механізмів координації та взаємодії між органами виконавчої влади;

в) планування та моніторинг виконання стратегічних цілей та пріоритетів КМУ;

г) забезпечення взаємодії КМУ з органами місцевого самоврядування, громадськістю та міжнародними організаціями.

Директорат публічної адміністрації є структурним підрозділом СКМУ, який відповідає за забезпечення ефективної діяльності органів виконавчої влади.

Основними завданнями Директорату є:

а) забезпечення реалізації державної політики у сфері публічної адміністрації;

б) розробка та впровадження механізмів реформування системи публічної адміністрації;

в) забезпечення реалізації державної політики у сфері кадрового забезпечення органів виконавчої влади;

г) забезпечення взаємодії КМУ з органами місцевого самоврядування, громадськістю та міжнародними організаціями у сфері публічної адміністрації.

Урядовий офіс координації європейської та євроатлантичної інтеграції (далі – УОЦЄАІ) є структурним підрозділом СКМУ, який відповідає за координацію діяльності органів виконавчої влади щодо реалізації Угоди про асоціацію між Україною та ЄС, а також за співробітництво з НАТО. Основними завданнями УОЦЄАІ є:

а) координація діяльності органів виконавчої влади щодо реалізації Угоди про асоціацію між Україною та ЄС;

б) підготовка та організація діяльності КМУ з питань європейської та євроатлантичної інтеграції;

в) забезпечення взаємодії КМУ з органами місцевого самоврядування, громадськістю та міжнародними організаціями у сфері європейської та євроатлантичної інтеграції.

Департамент з питань фінансового та економічного розвитку (далі – Департамент) є структурним підрозділом СКМУ, який відповідає за забезпечення реалізації державної політики у сфері фінансового та економічного розвитку. Основними завданнями Департаменту є:

а) забезпечення реалізації державної політики у сфері фінансового та економічного розвитку;

б) розробка та впровадження механізмів реформування фінансової та економічної системи;

в) забезпечення взаємодії КМУ з органами місцевого самоврядування, громадськістю та міжнародними організаціями у сфері фінансового та економічного розвитку.

Департамент з питань ефективного управління державною власністю є структурним підрозділом СКМУ, який відповідає за забезпечення реалізації державної політики у сфері ефективного управління державною власністю. Основними завданнями Департаменту є:

а) забезпечення реалізації державної політики у сфері ефективного управління державною власністю;

б) розробка та впровадження механізмів реформування системи управління державною власністю;

в) забезпечення взаємодії КМУ з органами місцевого самоврядування, громадськістю та міжнародними організаціями у сфері ефективного управління державною власністю.

Департамент з питань розвитку паливно-енергетичного комплексу та житлово-комунального господарства є структурним підрозділом СКМУ, який відповідає за забезпечення реалізації державної політики у сфері паливно-енергетичного комплексу та житлово-комунального господарства. Основними завданнями Департаменту є:

а) забезпечення реалізації державної політики у сфері паливно-енергетичного комплексу та житлово-комунального господарства;

б) розробка та впровадження механізмів реформування паливно-енергетичного комплексу та житлово-комунального господарства;

в) забезпечення взаємодії КМУ з органами місцевого самоврядування, громадськістю та міжнародними організаціями у сфері паливно-енергетичного комплексу та житлово-комунального господарства.

Департамент є важливим елементом системи забезпечення реалізації державної політики у сфері паливно-енергетичного комплексу та житлово-комунального господарства. Він забезпечує розробку та впровадження реформ у цій сфері, а також сприяє взаємодії між органами виконавчої влади та іншими учасниками суспільних відносин.

Департамент з питань безпеки, оборони, діяльності органів юстиції та запобігання корупції є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення реалізації державної політики у сферах безпеки, оборони, діяльності органів юстиції та запобігання корупції.

Основними завданнями Департаменту є:

а) надання інформації про воєнні злочини, вчинені російськими військами в Україні. Це включає інформацію про місця вчинення злочинів, типи злочинів, постраждалих та інших важливих деталях;

б) надання допомоги жертвам воєнних злочинів. Це включає допомогу в отриманні медичної допомоги, психологічної підтримки та інших видів допомоги.

Співпраця з міжнародними правоохоронними органами для притягнення винних до відповідальності. Це включає надання інформації та доказів про воєнні злочини, а також співпрацю з міжнародними організаціями, які допомагають вести розслідування. Департамент вирішує такі завдання:

а) веде збір інформації про воєнні злочини. Це включає роботу з очевидцями, жертвами, волонтерами та іншими джерелами інформації;

б) відповідає на запити про інформацію;

в) розслідує воєнні злочини;

г) поширює інформацію про воєнні злочини.

Департамент з питань безпеки життєдіяльності, охорони навколишнього природного середовища та агропромислового комплексу є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення реалізації державної політики у сферах безпеки життєдіяльності, охорони навколишнього природного середовища та агропромислового комплексу. Основними завданнями Департаменту є:

а) участь у розробці та реалізації державної політики у сфері безпеки життєдіяльності, зокрема у забезпеченні безпеки життєдіяльності населення України, у тому числі в умовах воєнного стану.

б) співпраця з органами охорони навколишнього природного середовища з метою охорони навколишнього природного середовища, зокрема у запобіганні забрудненню навколишнього середовища, у охороні природи та у відновленні природних ресурсів.

в) розвиток агропромислового комплексу, зокрема у забезпеченні продовольчої безпеки України, розвитку сільського господарства та у розвитку переробної промисловості.

Департамент є важливим елементом системи забезпечення реалізації державної політики у сферах безпеки життєдіяльності, охорони навколишнього природного середовища та агропромислового комплексу. Він забезпечує розробку та впровадження реформ у цих сферах, а також сприяє взаємодії між органами виконавчої влади та іншими учасниками суспільних відносин.

Департамент з питань інфраструктури та технічного регулювання є відповідальним за розробку та впровадження політики у сферах інфраструктури та технічного регулювання. Це включає такі завдання, як:

а) визначення стратегії розвитку цих сфер;

б) розробка та впровадження механізмів реформування цих сфер;

в) забезпечення розвитку інфраструктури України;

г) забезпечення технічного регулювання в Україні.

Департамент також співпрацює з іншими державними органами, органами місцевого самоврядування, а також з міжнародними організаціями у сферах інфраструктури та технічного регулювання. Ось деякі конкретні приклади діяльності Департаменту:

а) бере участь у розробці та реалізації державної політики у сфері інфраструктури, зокрема у забезпеченні розвитку інфраструктури України, у тому числі в умовах воєнного стану;

б) співпрацює з органами технічного регулювання з метою забезпечення технічного регулювання в Україні, зокрема у розробці та впровадженні технічних регламентів, у сертифікації продукції та у забезпеченні якості продукції.

Департамент відповідає за реалізацію державної політики у сферах транспорту, будівництва, містобудування, дорожнього господарства, житлово-комунального господарства, технічного регулювання.

Департамент співпрацює з такими органами, як Міністерство інфраструктури України, Міністерство розвитку громад, територій та інфраструктури України, Міністерство економіки України, Державна служба України з питань безпеки на транспорті, Державна архітектурно-будівельна інспекція України, Державна служба України з питань технічного регулювання та споживчої політики.

Департамент гуманітарної та соціальної політики є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення реалізації державної політики у сферах гуманітарної допомоги, соціальної політики, сім'ї та дітей, молоді та спорту, освіти, науки та інновацій. Ось деякі конкретні приклади діяльності Департаменту:

а) бере участь у розробці та реалізації державної політики у сфері гуманітарної допомоги, зокрема у забезпеченні гуманітарної допомоги постраждалим від воєнних дій в Україні, у тому числі в умовах воєнного стану.

б) співпрацює з органами соціальної політики з метою забезпечення соціальної захисту населення України, зокрема у наданні соціальних послуг, у соціальній підтримці малозабезпечених сімей та дітей, у соціальній адаптації та інтеграції осіб з інвалідністю.

в) займається розвитком молоді та спорту, зокрема у забезпеченні розвитку молодіжного руху, у сприянні розвитку фізичної культури та спорту.

г) забезпечує якісну освіту в Україні, зокрема у забезпеченні доступу до освіти, у забезпеченні якості освіти, у сприянні розвитку освіти.

д) підтримує науку та інновації, зокрема у забезпеченні розвитку науки, у сприянні розвитку інновацій.

Департамент комунікацій є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення ефективної взаємодії з засобами масової інформації, підтримання діалогових відносин з громадськістю та забезпечення відкритості та прозорості діяльності органів державної влади. Департамент займається забезпеченням взаємодії між органами виконавчої влади та засобами

масової інформації, сприяє інформуванню громадськості про діяльність органів державної влади та забезпечує доступ громадян до інформації про діяльність органів державної влади. Департамент комунікацій є відповідальним за реалізацію державної політики у сфері комунікацій. Зокрема, бере участь у розробці та реалізації державної політики у сфері комунікацій, зокрема у забезпеченні ефективної взаємодії з засобами масової інформації, у підготовці та проведенні прес-конференцій, у співпраці з засобами масової інформації; співпрацює з громадськими організаціями з метою підтримання діалогових відносин з громадськістю, зокрема у проведенні круглих столів, у співпраці з громадськими організаціями; забезпечує відкритість та прозорість діяльності органів державної влади, зокрема у публікації інформації про діяльність органів державної влади на вебсайтах, у проведенні відкритих засідань КМУ.

Департамент інформації та взаємодії з громадськістю (далі – ДІВГ) є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення реалізації державної політики у сфері комунікацій. ДІВГ займається забезпеченням взаємодії між органами виконавчої влади та засобами масової інформації, сприяє інформуванню громадськості про діяльність органів державної влади та забезпечує доступ громадян до інформації про діяльність органів державної влади. ДІВГ є відповідальним за реалізацію державної політики у сфері комунікацій. Діяльність ДІВГ полягає у розробці та реалізації державної політики у сфері комунікацій, зокрема у забезпеченні ефективної взаємодії з засобами масової інформації, у підготовці та проведенні прес-конференцій, у співпраці з засобами масової інформації; співпраці з громадськими організаціями з метою підтримання діалогових відносин з громадськістю, зокрема у проведенні круглих столів, у співпраці з громадськими організаціями; забезпеченні відкритості та прозорості діяльності органів державної влади, зокрема у публікації інформації про діяльність органів державної влади на вебсайтах, у проведенні відкритих засідань КМУ.

Департамент з питань міжнародного співробітництва є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення реалізації державної політики у сфері міжнародного співробітництва. Департамент займається розробкою та впровадженням реформ у цій сфері, а також сприяє взаємодії між органами виконавчої влади та міжнародними організаціями та іноземними державами. Зокрема, бере участь у розробці та реалізації державної політики у сфері міжнародного співробітництва, зокрема у забезпеченні співпраці України з Європейським Союзом та НАТО, у підготовці та проведенні міжнародних зустрічей та конференцій; співпрацює з міжнародними організаціями та іноземними державами з метою забезпечення співпраці України з ними, зокрема у реалізації міжнародних проектів та програм, у залученні міжнародної допомоги.

Департамент координації міжнародної технічної допомоги (далі – ДКМТД) є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення ефективної координації міжнародної технічної допомоги в Україні. ДКМТД займається координацією діяльності органів виконавчої влади, міжнародних організацій та донорів у сфері міжнародної технічної допомоги, а також сприяє ефективному використанню міжнародної технічної допомоги та забезпеченню її прозорості та підзвітності. ДКМТД є відповідальним за координацію міжнародної технічної допомоги в Україні у таких сферах, як: економіка, соціальна сфера, безпека, охорона навколишнього природного середовища, розвиток людського капіталу. ДКМТД також співпрацює з іншими державними органами, органами місцевого самоврядування, а також з міжнародними організаціями у сфері координації міжнародної технічної допомоги. Основними напрямами діяльності ДКМТД є:

а) розробка та реалізації державної політики у сфері координації МТД, зокрема, забезпечення ефективної координації діяльності органів виконавчої влади, міжнародних організацій та донорів у сфері Міжнародної технічної допомоги;

б) співпраця з міжнародними організаціями та донорами з метою забезпечення ефективної координації у сфері міжнародної технічної допомоги, зокрема у розробці стратегій та планів міжнародної технічної допомоги, у залученні міжнародних партнерів;

в) проведення аудитів ефективності міжнародної технічної допомоги, забезпечення її прозорості та підзвітності.

Департамент регіональної політики є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення реалізації державної політики у сфері регіонального розвитку. Департамент займається розробкою та впровадженням реформ у цій сфері, а також сприяє взаємодії між органами виконавчої влади та органами місцевого самоврядування. Виконує такі завдання:

а) розроблює та впроваджує державну політику регіонального розвитку. Міністерство розробляє державну стратегію регіонального розвитку, щорічні плани заходів щодо її реалізації, а також методологічне керівництво та координацію діяльності з підготовки регіональних стратегій розвитку. Крім того, Міністерство здійснює моніторинг стану реалізації державної стратегії регіонального розвитку та інших програм і проектів регіонального розвитку;

б) координує діяльність центральних і місцевих органів виконавчої влади у сфері регіонального розвитку, зокрема, забезпечує взаємодію з центральними і місцевими органами виконавчої влади та органами місцевого самоврядування з питань регіонального розвитку;

в) сприяє розвитку інфраструктури регіонів та міжрегіонального економічного співробітництва. Міністерство розробляє і здійснює заходи, спрямовані на розбудову інфраструктури регіонів, зокрема забезпечує оцінку та відбір на конкурсних засадах поданих Радою міністрів Автономної Республіки Крим, місцевими держадміністраціями інвестиційних програм і проектів регіонального розвитку, а також здійснює щорічне подання КМУ пропозицій щодо розподілу коштів державного фонду регіонального розвитку з переліком відповідних програм і проектів, що можуть виконуватися за його рахунок;

г) сприяє розвитку сільських територій. Міністерство розробляє та забезпечує виконання за участю інших органів виконавчої влади та органів місцевого самоврядування програм розвитку сільських територій, а також проводить моніторинг соціально-економічних та інших показників розвитку сільських територій;

д) розробляє пропозиції щодо підвищення ефективності механізмів стимулювання регіонального розвитку, подоланню депресивності регіонів та їх регіонального вирівнювання;

е) розробляє пропозиції щодо адаптації національного законодавства до положень та стандартів регіональної політики країн ЄС. Міністерство займається адаптацією національного законодавства до положень та стандартів регіональної політики країн ЄС, забезпечує взаємодію Міністерства з національними, регіональними та місцевими інституціями у сфері регіонального розвитку, а також готує пропозиції щодо реалізації міжнародних програм з питань регіонального розвитку та бере участь у їх впровадженні.

Департамент моніторингу та контролю є структурним підрозділом Секретаріату КМУ, який відповідає за забезпечення ефективного моніторингу та контролю за виконанням органами виконавчої влади рішень Кабінету Міністрів України. Департамент займається моніторингом та контролем за виконанням рішень КМУ, а також сприяє взаємодії між КМУ та органами виконавчої влади щодо виконання цих рішень.

Департамент моніторингу та контролю є відповідальним за моніторинг та контроль за виконанням рішень КМУ у таких сферах, як: економіка; соціальна сфера; безпека; охорона навколишнього природного середовища; розвиток людського капіталу. Департамент також співпрацює з іншими державними органами, органами місцевого самоврядування, а також з міжнародними організаціями у сфері моніторингу та контролю. Діяльність Департаменту спрямована на виконання таких завдань:

а) розробка та реалізація державної політики у сфері моніторингу та контролю, зокрема у забезпеченні ефективного моніторингу та контролю за виконанням рішень КМУ.

б) співпраця з органами виконавчої влади з метою забезпечення ефективного моніторингу та контролю за виконанням рішень КМУ, зокрема у проведенні перевірок виконання рішень КМУ.

в) сприяння підвищенню ефективності системи моніторингу та контролю за виконанням рішень КМУ, зокрема у розробці та впровадженні нових методів та інструментів моніторингу та контролю.

Департамент інформаційних технологій та безпеки (далі – ДІТБ) є важливим елементом системи забезпечення ефективного функціонування інформаційних систем органів виконавчої влади та за кібербезпеку у сфері державної влади. Він забезпечує функціонування інформаційних систем органів виконавчої влади, а також сприяє підвищенню рівня кібербезпеки у сфері державної влади. Діяльності ДІТБ спрямована на вирішення різнопланових проблем пов’язаних із захистом інформації у кірберпросторі. Зокрема, це стосується розробки та реалізації державної політики у сфері інформаційних технологій та безпеки, зокрема, у забезпеченні функціонування інформаційних систем органів виконавчої влади, у підвищенні рівня кібербезпеки у сфері державної влади; співпраці з органами виконавчої влади з метою забезпечення функціонування інформаційних систем органів виконавчої влади, зокрема, у проведенні аудитів інформаційних систем органів виконавчої влади; підвищення рівня кібербезпеки у сфері державної влади, зокрема, у розробці та впровадженні нових методів та інструментів кібербезпеки.

Юридичний департамент Секретаріату КМУ є одним із ключових підрозділів компанії, який відповідає за надання юридичної підтримки бізнес-діяльності Секретаріату КМУ в Україні та за кордоном. До основних завдань Юридичного департаменту Секретаріату КМУ належать:

а) забезпечення дотримання СКМУ чинного законодавства України та міжнародних правових норм;

б) захист інтересів Секретаріату КМУ в судових та інших правоохоронних органах;

в) участь у розробці та узгодженні юридичних документів, що стосуються діяльності Секретаріату КМУ.

г) представництво інтересів Секретаріату КМУ в переговорах з контрагентами.

Юридичний департамент Секретаріату КМУ складається з висококваліфікованих юристів, які мають досвід роботи в різних галузях права. Департамент постійно розвивається та вдосконалює свої навички, щоб надавати найкращу юридичну підтримку Секретаріату КМУ. Юридичний департамент СКМУ веде підготовку та узгодження договорів, угод та інших юридичних документів, пов’язаних з діяльністю Секретаріату КМУ; слідкує за дотриманням Секретаріатом КМУ трудового, податкового, митного тощо законодавства України; захищає інтереси Секретаріату КМУ в суперечках з контрагентами, органами державної влади та іншими суб’єктами права; представляє інтереси Секретаріату КМУ в міжнародних судових органах.

Департамент кадрового забезпечення (далі – ДКЗ) Секретаріату КМУ є одним із ключових підрозділів компанії, який відповідає за управління персоналом в Секретаріаті КМУ та за кордоном. ДКЗ Секретаріату КМУ здійснює планування потреби в персоналі Секретаріату КМУ; проведення набору та відбору персоналу; оформлення трудових відносин з працівниками Секретаріату КМУ; сприяє розвитку та навчанню персоналу Секретаріату КМУ; управляє кар’єрою персоналу Секретаріату КМУ; забезпечує дотримання Секретаріатом КМУ трудового законодавства та інших нормативно-правових актів у сфері праці; здійснює управління заробітною платою та соціальними гарантіями персоналу Секретаріату КМУ; сприяє забезпеченню соціальної та психологічної підтримки персоналу Секретаріату КМУ.

Департамент організації засідань КМУ та урядових комітетів (далі – ДОЗКМУ) є одним із ключових підрозділів Секретаріату КМУ, який відповідає за організацію та проведення засідань КМУ та урядових комітетів. До основних завдань ДОЗКМУ належить опрацювання порядку денного засідань КМУ та урядових комітетів; запрошення учасників засідань КМУ та урядових комітетів; підготовка матеріалів для розгляду на засіданнях КМУ та урядових комітетів; організація проведення засідань КМУ та урядових комітетів; ведення протоколів засідань КМУ та урядових комітетів.

Департамент забезпечення документообігу є одним із ключових підрозділів компанії, який відповідає за організацію та забезпечення ефективного документообігу в компанії. до основних завдань належить:

а) розробка та впровадження єдиної системи документообігу в компанії, яка відповідає вимогам законодавства України та міжнародних стандартів;

б) забезпечення дотримання в компанії правил та процедур документообігу, затверджених керівництвом компанії;

в) організація прийому, реєстрації, обробки, зберігання та передачі документів в компанії в установленому порядку;

г) забезпечення доступу до документів працівникам компанії в установленому порядку;

д) забезпечення захисту документів від несанкціонованого доступу, втрати або знищення.

Департамент з питань взаємодії з Верховною Радою України, іншими державними органами є одним із ключових підрозділів Секретаріату КМУ. До основних завдань ДВВРУ належить опрацювання та аналіз законопроектів, інших нормативно-правових актів, які надходять до КМУ від ВРУ, інших державних органів та громадськості; підготовка та надання КМУ пропозицій щодо внесення змін до законопроектів, інших нормативно-правових актів; участь у переговорах КМУ з ВРУ, іншими державними органами та

громадськістю; проведення аналітичних досліджень з питань взаємодії КМУ з ВРУ, іншими державними органами та громадськістю.

Господарсько-фінансовий департамент (далі – ГФД) відповідає за управління фінансами та майном. Основні завдання ГФД полягають у формуванні бюджету компанії на основі прогнозів продажів, витрат та інвестицій; контролі за виконанням бюджету компанії; забезпеченні ефективного управління грошовими потоками, дебіторами та кредиторами, активами та пасивами компанії, дотриманні фінансової дисципліни.

Управління протоколу Секретаріату КМУ є одним із ключових підрозділів Секретаріату, який відповідає за організацію та проведення офіційних зустрічей, конференцій та інших заходів, участь у яких бере прем'єр-міністр України, інші члени Уряду, а також закордонні делегації; планування та організація офіційних зустрічей, конференцій та інших заходів, участь у яких бере прем'єр-міністр України, інші члени Уряду, а також закордонні делегації. З метою дотримання Протоколу Управління готує та розсилає запрошення на заходи; організовує реєстрації учасників таких заходів; забезпечує проведення таких заходів відповідно до встановлених правил і процедур; веде протоколи заходів.

Управління з питань роботи із зверненнями громадян (далі – УЗРГ) – це підрозділ Секретаріату КМУ, який відповідає за організацію та забезпечення ефективного розгляду звернень громадян. До основних завдань УЗРГ належать:

а) прийом звернень громадян у письмовій, усній та інших формах;

б) реєстрація звернень громадян відповідно до вимог законодавства України;

в) опрацювання звернень громадян з метою встановлення їхнього змісту та визначення відповідальної за розгляд структури Секретаріату;

г) направлення звернень громадян до відповідальної за розгляд структури Секретаріату.

д) контроль за розглядом звернень громадян відповідальною за розгляд структурою Секретаріату;

е) забезпечення надання відповідей на звернення громадян у встановленому порядку;

ж) проведення аналізу звернень громадян з метою виявлення проблемних питань та розробки пропозицій щодо їх вирішення;

к) сприяння взаємодії КМУ з громадянами у вирішенні їхніх проблем.

Режимно-секретне управління (далі – РСУ) – це спеціальний підрозділ в органах державної влади та місцевого самоврядування, який відповідає за організацію та забезпечення захисту державної таємниці. До основних завдань РСУ належить:

а) розробка та затвердження нормативно-правових актів з питань режиму секретності;

б) організація та проведення інструктажів з питань режиму секретності для працівників органів державної влади та місцевого самоврядування;

в) надання консультацій з питань режиму секретності;

г) проведення перевірок стану режиму секретності в органах державної влади та місцевого самоврядування;

д) внесення пропозицій щодо вдосконалення системи захисту державної таємниці.

Управління організаційно-аналітичного забезпечення діяльності прем'єр-міністра України (далі – УОАЗ) відповідає за організацію та забезпечення ефективного виконання прем'єр-міністром України його повноважень. До основних завдань УОАЗ належать:

а) організація засідань КМУ, інших колегіальних органів, які очолює прем'єр-міністр;

б) організація робочих поїздок прем'єр-міністра України;

в) складання та підготовка документів, необхідних для виконання повноважень прем'єр-міністром України;

г) забезпечення інформаційно-аналітичного забезпечення діяльності прем'єр-міністра України;

д) забезпечення взаємодії прем’єр-міністра України з іншими органами державної влади, місцевого самоврядування та міжнародними організаціями.

Відділ з питань дотримання антикорупційного законодавства Секретаріату КМУ відповідає за забезпечення дотримання антикорупційного законодавства в діяльності КМУ. До основних завдань Відділу належать:

а) розробка та затвердження нормативно-правових актів з питань запобігання корупції в діяльності КМУ;

б) організація та проведення навчальних заходів з питань антикорупції для працівників КМУ;

в) надання консультацій працівникам КМУ з питань антикорупційного законодавства;

г) взаємодія з органами державної влади та іншими суб’єктами, які здійснюють боротьбу з корупцією.

Відділ з питань санкційної політики Секретаріату КМУ відповідає за забезпечення реалізації санкційної політики України. До основних завдань Відділу належить координація діяльності центральних органів виконавчої влади з розробки та реалізації заходів щодо застосування санкцій; розробка пропозицій щодо застосування санкцій; моніторинг стану застосування санкцій; виконання міжнародних зобов’язань України у сфері санкційної політики.

Сектор мобілізаційної роботи Секретаріату КМУ є підрозділом Секретаріату, який відповідає за організацію та забезпечення мобілізаційної підготовки та мобілізації в Україні. До основних завдань Сектора належить координація діяльності центральних органів виконавчої влади з розробки та реалізації заходів щодо мобілізаційної підготовки та мобілізації; розробка пропозицій щодо мобілізаційної підготовки та мобілізації; моніторинг стану мобілізаційної готовності держави; виконання міжнародних зобов’язань України у сфері мобілізаційної підготовки та мобілізації.

Сектор внутрішнього аудиту Секретаріату КМУ є підрозділом Секретаріату, який відповідає за проведення внутрішніх аудитів діяльності

Секретаріату та його структурних підрозділів. Завданнями Сектора є планування та проведення внутрішніх аудитів діяльності Секретаріату та його структурних підрозділів; надання рекомендацій щодо удосконалення діяльності Секретаріату та його структурних підрозділів; моніторинг виконання рекомендацій, наданих за результатами внутрішніх аудитів; виконання міжнародних зобов'язань України у сфері внутрішнього аудиту.

Секретаріат КМУ є центральним органом виконавчої влади, який забезпечує діяльність КМУ. У своїй діяльності Секретаріат обробляє значну кількість інформації, в тому числі конфіденційної та секретної. Тому питання забезпечення її захисту є одним із пріоритетних для Секретаріату.

Отже, Секретаріат КМУ має розгалужену структуру, завдання якої полягає у створенні умов для ефективної роботи КМУ. Одним із важливих напрямів діяльності Секретаріату КМУ є організація захисту інформації, у тому числі у кіберпросторі, що особливо важливо під час війни, зокрема введений режим секретності на всіх рівнях. Кожна з структур при виконанні своїх обов'язків діє відповідно до норм, які посилюють інформаційну безпеку у сфері державного управління.

3.2. Захист інформації в Секретаріаті КМУ

Захист інформації в Секретаріаті КМУ здійснюється відповідно до законодавства України, зокрема Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3], Закону України «Про державну таємницю» та інших нормативно-правових актів. [22]

Основними завданнями захисту інформації в Секретаріаті КМУ є запобігання несанкціонованому доступу до інформації, її копіюванню, спотворенню, знищенню або поширенню; порушенню цілісності та достовірності інформації.

Для забезпечення цих завдань у Секретаріаті КМУ реалізуються наступні заходи:

а) розроблення та впровадження нормативно-правових актів та методичних документів з питань захисту інформації;

б) проведення навчання працівників Секретаріату з питань захисту інформації;

в) створення та впровадження технічних засобів захисту інформації;

г) здійснення контролю за станом захисту інформації.

У Секретаріаті КМУ розроблено та впроваджено комплексну систему захисту інформації, яка включає в себе наступні компоненти:

а) організаційний захист;

б) технічний захист;

в) програмний захист.

Організаційний захист передбачає розроблення та впровадження відповідних організаційних заходів, спрямованих на забезпечення захисту інформації. До таких заходів належать:

а) визначення та класифікація інформації;

б) встановлення порядку доступу до інформації;

в) організація роботи з документами, що містять інформацію з обмеженим доступом;

г) проведення інструктажів з питань захисту інформації для працівників Секретаріату.

Технічний захист передбачає використання технічних засобів, призначених для захисту інформації від несанкціонованого доступу, копіювання, зміни, знищення або поширення. До таких засобів належать:

а) системи фізичного захисту;

б) системи контролю доступу;

в) системи виявлення та попередження про несанкціонований доступ;

г) системи криптографічного захисту інформації.

Програмний захист передбачає використання програмних засобів, призначених для захисту інформації від несанкціонованого доступу, копіювання, зміни, знищення або поширення. До таких засобів належать: антивірусні програми; програми для захисту від шкідливого програмного забезпечення; програми для захисту від несанкціонованого доступу до інформації.

Заходи із захисту інформації в Секретаріаті КМУ є постійною та комплексною роботою, спрямованою на забезпечення безпеки інформації, яка обробляється в Секретаріаті.

Слід зауважити, що інформаційна діяльність в Секретаріаті КМУ регламентується постановою «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтого 2016 р., №736 [17]. Відповідно до 4 пункту зазначеної вище постанови був розроблений наказ «Про затвердження Порядку роботи в Секретаріаті Кабінету Міністрів України з документами та іншими матеріальними носіями інформації, що містять службову інформацію», який містить інформацію щодо службового користування. Така інформація носить конфіденційний характер, тому доступу до неї не було надано.

Якщо говорити про технологічні засоби захисту інформації то потрібно згадати про використання автономних комп’ютерів. Для захисту таких комп’ютерів від несанкціонованого доступу в Секретаріаті КМУ застосовуються такі заходи:

а) фізичний захист: автономні комп’ютери зберігаються в захищених приміщеннях, доступ до яких обмежений;

б) програмний захист: на автономних комп’ютерах, мережевому обладнанні, встановлюються антивірусні програми та інші засоби захисту від шкідливого програмного забезпечення.

Організаційні заходи: персонал, який працює з автономними комп’ютерами, проходить навчання з питань інформаційної безпеки.

Отже, в Секретаріаті КМУ захист інформації проводиться на організаційному, технологічному та програмному рівні, які регламентовані законодавчою та нормативною базою.

Таким чином, у цьому розділі була проаналізовано роботу структурних підрозділів Секретаріат КМУ, у рамках того обсягу інформації до якої має доступ цивільна людина під час війни. Для забезпечення інформаційної безпеки Секретаріат КМУ спирається на ті самі закони що використовують інші державні установи чи організації, але через специфіку установи та рівні секретності може мати свої аналоги для внутрішнього користування, який не розголошується простим людям. Якщо говорити про технічне забезпечення інформаційної безпеки, то Секретаріат має свої системи захисту які включають як перестрахування, в плані автономних комп’ютерів, так і постійне забезпечення установи новими засобами захисту, такі як специфічне програмне забезпечення та апаратуру.

ВИСНОВКИ

Захист інформації є важливим завданням для будь-якої людини чи організації, в тому числі і для Секретаріату Кабінету Міністрів України. У сучасних умовах, коли інформаційні технології є невід'ємною частиною захист інформації та життєдіяльності суспільства, загрози інформаційній безпеці зростають. Для підвищення рівня захисту інформації необхідно вживати комплекс заходів, включаючи впровадження сучасних технічних засобів, розробку ефективних організаційних та програмних заходів захисту інформації та підвищення рівня обізнаності з питань захисту інформації.

У рамках даного дослідження було проведено аналіз наукових статей за останні роки, які висвітлювали різні аспекти інформаційної безпеки в Україні. На прикладі таких статей, «Загрози інформаційній безпеці України як проблематика національної безпеки», «Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктриний законодавчої основи», чи «Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти». Під час аналізу цих статей було зазначено що ближче до сучасного часу, вчені все більше використовували аспект пов'язаний з іт-технологіями, а саме кібербезпеку, тобто захист інформації в технологічному просторі. Водночас питання захисту інформації у аналізованих статтях підняло інтерес як проходить організація захисту інформації в органах влади, зокрема в Секретаріаті Кабінету Міністрів України, що має свою специфіку у сьогоднішній час. Також була встановлена різниця, між поняттями інформаційною безпекою, яка визначає стан захищеності інформацію, захистом інформацій, який розповідає про методи та методики, та кібербезпекою які є складовою захисту інформації в нових технологіях.

Також в цьому розділі було розглянуто низку законів та нормативно-правових актів які забезпечують організацію захисту інформації, як в державі, так і ті закони що допомагають в забезпеченні інформаційної безпеки, або

регулюють цю сферу у специфічних питаннях або у військовий час. Роблячи висновок, можна чітко казати що правовий аспект інформаційної безпеки завжди поповнюється правками, або стратегіями для подальшого запобігання можливим та явним загрозам.

Було охарактеризовано важливість ролі та загрози в захисті інформації під час діяльності установ та організацій, та взагалі важливість розширення знань у цій сфері, бо це важливо для всіх сфер населення, та кожного кроку в діяльності з інформацією, яка може підпадати під різні рівні конфіденційності в установах та компаніях, та важливість для особи, розголошення якої може бути використано для завдання шкоди.

В кваліфікаційній роботі розглянуті вимоги до забезпечення захисту інформації в Секретаріаті Кабінету Міністрів України. Було встановлено, що ця державна установа має різні рівні секретності, тому більшість інформації відноситься до державної таємниці, або є конфіденційною. Кожний структурний підрозділ має свої системи захисту та рівні конфіденційної інформації. З'ясовано, що інформаційна безпека в Секретаріаті Кабінету Міністрів України здійснюється відповідно до законодавства України, як в межах нормативно-правових актів, так і визначається внутрішніми нормативними документами, які призначенні для внутрішнього користування та не розголошуються. Отже, інформаційна безпека в даній установі є комплексною та застосовується для захисту інформації та паперових носіях, так і електронних. Особливої уваги надається захисту комп'ютерів від несанкціонованого втручання.

Також було встановлено, що партнерство у сфері захисту інформації є важливим фактором забезпечення інформаційної безпеки в Україні. Воно передбачає співпрацю між різними суб'єктами інформаційної діяльності, зокрема органами державної влади, органами місцевого самоврядування, профільними установами та організаціями, а також міжнародними організаціями. Зазначено що Україна веде партнерство з іншими закордонними партнерами, такими як ООН, ОБСЕ, НАТО, ЕС.

СПИСОК ВИКОРИСТНИХ ДЖЕРЕЛ

Законодавчі та нормативно-правові акти

1. Конституція України від 28.06.1996, № 30, ст. 141 Поточна редакція 01.01.2020. База даних «Законодавство України». URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 10.07.2023.)

2. Про інформацію: Закон України від 02.10.1992. Поточна редакція 31.03.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.07.2023.)

3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994. Поточна редакція 01.07.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 10.07.2023.)

4. Про створення єдиної системи залучення, використання та моніторингу міжнародної технічної допомоги: Постанова Каб. Міністрів України від 15.02.2002. Поточна редакція 25.08.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/153-2002-п#Text

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. Поточна редакція 17.08.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006. Поточна редакція 31.03.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

7. Про критичну інфраструктуру: Закон України від 16.11.2021. Поточна редакція 05.12.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

8. Про електронні документи та електронний документообіг: Закон України від 22.05.2003. Поточна редакція 01.08.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

9. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури: Постанова Каб. Міністрів України від 24.03.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/257-2023-п#Text

10. Про національну безпеку України: Закон України від 21.06.2018. Поточна редакція 31.03.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 15.09.2023).

11. Про основи національної безпеки України: Закон України від 19.06.2003. Поточна редакція 08.07.2018. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 15.09.2023).

12. Про правовий режим воєнного стану: Закон України від 12.05.2015. Поточна редакція 20.08.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 12.10.2023).

13. Про Національну поліцію: Закон України від 02.07.2015. Поточна редакція 05.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 12.10.2023).

14. Про Службу безпеки України: Закон України від 25.03.1992 р. Поточна редакція 02.08.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 12.10.2023).

15. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016. Поточна редакція 17.07.2021. База даних

«Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 12.10.2023).

16. Про введення воєнного стану в Україні: Указ Президента України від 26.11.2018. Поточна редакція 28.11.2018. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/393/2018#Text (дата звернення: 12.10.2023).

17. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію: Постанова Каб. Міністрів України від 19.10.2016. Поточна редакція 25.08.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/736-2016-п#Text (дата звернення: 12.10.2023).

18. Про затвердження Положення про Секретаріат Кабінету Міністрів України: Постанова Каб. Міністрів України від 12.08.2009. Поточна редакція 30.08.2020. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/850-2009-п#Text (дата звернення: 08.10.2023).

19. Про затвердження структури Секретаріату Кабінету Міністрів України: Постанова Каб. Міністрів України від 23.08.2016. Поточна редакція 16.03.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/564-2016-п#Text (дата звернення: 08.10.2023).

20. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021.. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

21. Про затвердження Регламенту Кабінету Міністрів України: Постанова Каб. Міністрів України від 18.07.2007. Поточна редакція 11.05.2023. База даних

«Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/950-2007-п#Text (дата звернення: 31.10.2023).

22. Про державну таємницю: Закон України від 21.01.1994. Поточна редакція 31.03.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 01.11.2023).

Наукові, довідкові та навчальні видання

23. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. *Державне управління: удосконалення та розвиток*. 2019. URL: http://www.dy.nayka.com.ua/?op=1&z=1528 (дата звернення: 10.08.2023).

24. Баранов О. А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти*: матеріали наук.-практ. конф. м. Київ, 6 жовт. 2016 р. / упоряд. В. М. Фурашев. Київ: Вид-во «Політехніка», 2016. С. 29–35.

25. Біленчук П. Д. Правові засади інформаційної безпеки України: монографія / П. Д. Біленчук, Л. В. Борисова, І. М. Неклонський., В. О. Собина; за ред. П. Д. Біленчука Харків: 2018. 289 с.

26. Валюшко І. Інформаційна безпека України: трансформація законодавства після російського вторгнення. URL: https://core.ac.uk/download/pdf/197266255.pdf. (дата звернення: 10.08.2023).

27. Візир Т. Адміністративно-правове регулювання забезпечення інформаційної безпеки в Україні: сучасний стан та перспективи вдосконалення. *International electronic scientific journal «Science Online»*. 2019. № 4. URL: https://doi.org/10.25313/2524-2695-2019-4-administrativno-pravove-regulyuvannya-zabezpechennya-informatsijnoyi-bezpeki-v-ukrayini-suchasnij-stan-ta-perspektivi-vdoskonalennya (дата звернення: 10.08.2023).

28. Вітер С. А, Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Мукач. держ. ун-т. С. 497–502. url: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (дата звернення: 10.08.2023).

29. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна*. Сер.: Право. 2020. Вип. 29. С. 281–288.
URL: https://dspace.univd.edu.ua/items/9db62c35-e646-4273-a19b-821ed36c4aeb (дата звернення: 10.08.2023).

30. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. 2018. № 53. С. 26–37. URL: http://easternlaw.com.ua/wp-content/uploads/2018/07/voytsikhovskyy_53.pdf. (дата звернення: 10.08.2023).

31. Виздрик В., Мельник О. Інформаційна безпека в україні: сучасний стан. *Grail of science*. 2023. № 24. С. 196–202. URL: https://archive.journal-grail.science/index.php/2710-3056/article/view/867 (дата звернення: 10.08.2023).

32. Гаврильців М. Т. Інформаційна безпека держави у системі національної безпеки України. *Юридичний науковий електронний журнал.* 2020. № 2. С. 200–203. URL: http://lsej.org.ua/2_2020/54.pdf (дата звернення: 10.08.2023).

33. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення ін-формаційної безпеки України. *Науковий вісник Ужгородського національного університету.* Серія ПРАВО. 2022. № 70. С. 24–27. URL: https://doi.org/10.24144/2307-3322.2022.70.3 (дата звернення: 31.10.2023).

34. Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання. *Вісн. УАДУ*. 2002. № 3. С. 27–31.

35. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки. Київ: Видавництво НА СБ України. 2020. 256 с.

36. Інформаційна безпека і кібербезпека – в чому різниця? *Wayback Machine*. URL: https://web.archive.org/web/20191017165559/https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/ (дата звернення: 01.10.2023).

37. Інформаційна безпека. *Фармацевтична енциклопедія*. URL: https://www.pharmencyclopedia.com.ua/article/8023/informacijna-bezpeka (дата звернення: 31.10.2023).

38. Інформаційна безпека. *Енциклопедія Сучасної України ЕСУ*. URL: https://esu.com.ua/search_articles.php?id=12457 (дата звернення: 31.10.2023).

39. Інформаційна безпека: види загроз і методи їх усунення. *datami*. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 31.10.2023).

40. Інформаційна безпека. *Wise IT Ukraine*. URL: https://wiseit.com.ua/services/rishennya-ta-servisy/informaczijna-bezpeka/ (дата звернення: 31.10.2023).

41. Інформаційна безпека працівників: важливі правила, які варто враховувати. *TechExpert*. URL: https://techexpert.ua/employees-cyber-security-at-work/ (дата звернення: 31.10.2023).

42. IT-безпека та інформаційна безпека – у чому різниця? *DQS | Audits und Zertifizierung | Simply leveraging Quality*. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/it-bezpeka-ta-informacijna-bezpeka-–-u-chomu-riznicya (дата звернення: 04.10.2023).

43. Давидюк А. Зубок В, Хохлачова Ю., Худинцев М., Комаров М. Кіберстатистика в україні. сучасний стан. *Ukrainian scientific journal of*

information security. 2023. Т. 29. № 2. С. 53–60. URL: https://doi.org/10.18372/2225-5036.29.17868 (дата звернення: 30.10.2023).

44. Довгань О. Д., Ткачук Т. Ю., Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1(28). С. 86–99. URL: https://ippi.org.ua/sites/default/files/12_11.pdf (дата звернення: 10.08.2023).

45. Залєвська І. І., Удренас Г. І. Інформаційна безпека україни в умовах російської військової агресії. *South Ukrainian Law Journal*. 2022. № 1-2. С. 20–26. URL: https://doi.org/10.32850/sulj.2022.1-2.4 (дата звернення: 10.08.2023).

46. Зозуля О.С. Періодизація розбудови системи державного управління забезпеченням інформаційної безпеки України. *Інвестиції: практика та досвід*. Київ., 2016. №8. С. 106–114.

47. Даник Ю., Воробієнко П., Чернега В. Основи кібербезпеки та кібероборони. 2-ге вид. Одеса: ОНАЗ ім. О.С. Поп., 2019. 320 с.

48. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О. О. Захист інформації в комп'ютерних системах: підручник., 12-те вид. Ніжин: ФОП Лук'яненко В. В., ТПК «Орхідея», 2020. 236 с.

49. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. №1. С. 150–155. URL: https://doi.org/10.32782/392257 (дата звернення: 10.08.2023).

50. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування. Житомир: Видавець ПП «Євро-Волинь», 2021. 172 с.

51. Леоненко Н. А., Поступна О. В. Інформаційна безпека україни: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Bulletin of the national university of civil protection of ukraine. series: public administration*. 2022. Issue 2(17)2022. URL: https://doi.org/10.52363/2414-5866-2022-2-14 (дата звернення: 15.08.2023).

52. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навч. по-сіб. / В.А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с.

53. Лісовська Ю. Інформаційна безпека України. Київ: Кондор, 2018. 172 с.

54. Мазепа С. О. Інформаційна безпека в умовах війни. Російсько-українська війна: право, безпека, світ. 2022. С. 237–238. URL: http://confuf.wunu.edu.ua/index.php/confuf/article/view/942/924 (дата звернення: 15.09.2023)

55. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. № 1(40). С. 111–118. URL: https://doi.org/10.37750/2616-6798.2022.1(40).254349 (дата звернення: 10.08.2023).

56. Невельська-Гордєєва О., Нечитайло В. Феномен «fake news» в контексті забезпечення інформаційної безпеки держави. *Вісник НЮУ імені Ярослава Мудрого*. Серія: Філософія, філософія права, політологія, соціологія. 2022. Т. 1. № 52. URL: https://doi.org/10.21564/2663-5704.52.250655 (дата звернення: 31.10.2023).

57. Основи кібергігієни. *Дія.Освіта*. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 10.10.2023).

58. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки». 2021. Т. 8. № 31. С. 167–179. URL: https://doi.org/10.23939/law2021.31.167 (дата звернення: 10.08.2023).

59. Панченко О. Інформаційна Складова Національної Безпеки. *Вісник Національної академії Державної прикордонної служби України*. 2019. № 3. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf. (дата звернення: 15.09.2023).

60. Петров В. В. Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн: автореферат дис. канд. політ. наук: 21.01.01 / В. В.

Петров ; Рада нац. безпеки і оборони України, Нац. ін-т пробл. міжнар. безпеки. Київ. 2010. 20 с.

61. Петрик В. М. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал.* 2009. № 5. URL: http://www.justinian.com.ua/article.php?id=3222 (дата звернення: 15.09.2023).

62. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. *Сучасний захист інформації*. 2015. № 4. С. 86–90.

63. Піддубна Л. В., Павліченко В. М. Інформаційна безпека в системах електронного документообігу. *Науковий вісник Полтавського університету економіки і торгівлі*. 2020. № 4 (95). URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvpusk_2019_4_10 (дата звернення: 24.10.2023).

64. Поняття та зміст інформаційної безпеки. *Національна безпека України: навчальний посібник*. *Політологія: Онлайн бібліотека.* URL: http://politics.ellib.org.ua/pages-8280.html (дата звернення: 31.10.2023).

65. Про нас. *Офіційний вебсайт Міністерства цифрової трансформації України.* URL: https://thedigital.gov.ua/ministry (дата звернення: 12.10.2023).

66. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Scientific works of national aviation university. series: law journal "air and space law"*. 2021. Т. 2. № 59. С. 110–115. URL: https://doi.org/10.18372/2307-9061.59.15603 (дата звернення: 30.10.2023).

67. Сніцаренко П. М., Саричев Ю. О., Семененко В. М., Ткаченко В. А. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. *Збірник наукових праць Центру воєнностратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 2(63). С. 68–74.

68. Системи інформаційної безпеки. *ProNET*.

URL: https://pronet.ua/sistemi-informaczijnoi-bezpeki/ (дата звернення: 05.10.2023).

69. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186. URL: http://pgp-journal.kiev.ua/archive/2017/10/38.pdf (дата звернення: 14.08.2023)

70. Ткаченко В. В., Паливода В. В. Загрози інформаційній безпеці України як проблематика національної безпеки. *Юридичний науковий електронний журнал.* 2022. № 10. С. 496–498. URL: https://doi.org/10.32782/2524-0374/2022-10/123 (дата звернення: 25.10.2023).

71. Черниш Р. Ф., Ігнатюк М. В., Заріцький О. Ю. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал.* 2022. № 1. С. 213–216. URL: https://doi.org/10.32782/2524-0374/2022-1/54 (дата звернення: 15.08.2023).

72. Чалапко В. Інформаційна безпека: до проблеми місця й ролі у системі національної безпеки. *Вісник НЮУ імені Ярослава Мудрого.* Серія: Філософія, філософія права, політологія, соціологія. 2021. Т. 4. № 51. URL: https://doi.org/10.21564/2663-5704.51.242004 (дата звернення: 01.11.2023).

73. Шемчук В. В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз. Київ: Ліра-К, 2022. 352 с.

74. Шемчук В. В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктриний законодавчої основи. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія: Юридичні науки. 2019. Т 30(69). № 4. С. 31–37. URL: https://www.juris.vernadskyjournals.in.ua/journals/2019/4_2019/8.pdf

75. Шульженко Н. В. Інформаційна безпека від загроз транснаціональної організованої злочинності. *Аналітично-порівняльне правознавство*. 2023. № 6.

С. 307–310. URL: https://doi.org/10.24144/2788-6018.2022.06.55 (дата звернення: 31.10.2023).

76. Що таке інформаційна безпека. *Resit*.

URL: https://resit.com.ua/sho-take-informazijna-bezpeka-kompanii/ (дата звернення: 31.10.2023).

77. Що таке інформаційна безпека підприємства та які основні засади захисту даних існують? *iIT Distribution*. URL: https://iitd.com.ua/news/shho-take-informacijna-bezpeka-pidpriiemstva-ta-jaki-osnovni-zasadi-zahistu-danih-isnujut/ (дата звернення: 31.10.2023).

78. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія Право. 2016. № 2. С. 244–252.

79. Яковлєв П. О. Об'єкт і предмет державного регулювання у сфері забезпечення інформаційної безпеки України. *Право і суспільство*. 2020. № 3. С. 178–183. URL: https://doi.org/10.32842/2078-3736/2020.3.27 (дата звернення: 01.11.2023).

80. Методичний підхід до управління ризиками безпеки інформації як складової забезпечення інформаційної безпеки держави / П. Сніцаренко та ін. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського*. 2022. С. 47–55. URL: https://doi.org/10.33099/2304-2745/2022-2-75/47-55 (дата звернення: 01.11.2023).

ДОДАТКИ

ДОДАТОК А

Таблиця 2 – Підходи до визначення поняття «інформаційної безпеки» [23]

Автор	Визначення
А. Тер-Акопов	стан захищеності інформації, що забезпечує життєво важливі інтереси людини
О. Возженніков, В. Калайда, Ю. Максименко, О. Прохожев, Т. Філіпенко, А. Юричко	стан, що характеризується відсутністю загроз, тобто чинників і умов, котрі несуть загрозу безпосередньо індивідові, суспільству, державі з боку інформаційного середовища
Я. Серебренніков	діяльність людей, суспільства, держави, світової спільноти із виявлення (вивчення), попередження, ослаблення, усунення (ліквідації) викликів і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної (неприпустимої об'єктивно і суб'єктивно) шкоди, закрити шлях для прогресивного розвитку
І. Панарін	стан захищеності інформаційного середовища, що відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від дії внутрішніх і зовнішніх інформаційних загроз
Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»	стан захищеності життєвоважливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації
Закон України «Про телекомунікації»	стан захищеності основних інтересів особистості, суспільства і держави у сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота, об'єктивність, доступність і конфіденційність. Головна відмінність інформаційної безпеки полягає в тому, що, будучи складовою національної безпеки, вона є невід'ємною складовою інших її складових: економічної безпеки, воєнної безпеки, політичної безпеки тощо.

ДОДАТОК Б

ПЕРЕДДИПЛОМНА РОБОТА В СЕКРЕТАРІАТІ КМУ

Національний авіаційний університет
Факультет лінгвістики та соціальних комунікацій
Кафедра історії та документознавства

ЩОДЕННИК
з переддипломної практики у сфері
документознавства та інформаційної діяльності

в Секретаріаті Кабінету Міністрів України, Департамент забезпечення документообігу, Відділ випуску актів Кабінету Міністрів України та організації роботи урядового архіву

Здобувача вищої освіти ДК 621 групи
СЛЮСАР Ігор Володимирович
(прізвище, ім'я та по-батькові студента)
ОС «Магістр»
Галузь знань: 02 «Культура і мистецтво»
Спеціальність 029 «Інформаційна, бібліотечна та архівна справа»
Освітньо-професійна програма «Документознавство та інформаційна діяльність»

з 01 вересня по 24 вересня 2023

Керівник від Національного авіаційного університету
завідувач кафедри ТЮРМЕНКО Ірина Іванівна
(підпис) (посада, прізвище, ім'я, по-батькові)

Керівник від бази практики
Завідуюча відділом випуску актів Кабінету Міністрів України та організації роботи урядового архіву Кривиленко Світлана Миколаївна.
(підпис) (посада, прізвище, ім'я, по-батькові)

Прибув на базу практики в СКМУ
01.09.2023 (назва бази практики)
Печатка
бази практики « » 2023року
_____ завідуюча відділом випуску актів Кабінету Міністрів України та організації роботи урядового архіву Кривиленко Світлана Миколаївна.
(підпис) (посада, прізвище та ініціали відповідальної особи)

Вибув з бази практики в СКМУ:
22.09.2022 (назва бази практики)
Печатка
бази практики «___» _____2023 року

_____ завідуюча відділом випуску актів Кабінету Міністрів України та організації роботи урядового архіву Кривиленко Світлана Миколаївна.
(підпис) (посада, прізвище та ініціали відповідальної особи)

Робочі записи під час практики

дата	Що зроблено	Підпис керівника практики
01.09.2023 09:00-15:00	1. Настановча конференція на базі проведення практики. 2. Інструктаж з техніки безпеки. 3. Знайомство з базою практики.	
02.09.2023 09:00-15:00	Огляд загальної структури Секретаріату Кабінету Міністрів України	
03.09.2023 09:00-15:00	Аналіз нормативно-правової бази про структуру Секретаріату Кабінету Міністрів України	
04.09.2023 09:00-15:00	Аналіз структурних підрозділів керуючої ланки Секретаріату Кабінету Міністрів України	
05.09.2023 09:00-15:00	Аналіз структурних підрозділів Секретаріату Кабінету Міністрів України	
06.09.2023 09:00-15:00	Праця з кваліфікаційною роботою. (Структура і робота Секретаріату Кабінету Міністрів України)	
07.09.2023 09:00-15:00	Завершення аналізу структурних підрозділів Секретаріату Кабінету Міністрів України	
08.09.2023 09:00-15:00	Аналіз нормативно-правової бази захисту інформації в Україні	
09.09.2023 09:00-15:00	Праця з кваліфікаційною роботою. (Список нормативно-правової бази захисту інформації в Україні)	
10.09.2023 09:00-15:00	Оформлення кінцевого змісту завдання з нормативно-правової бази захисту інформації в Україні	
11.09.2023 09:00-15:00	Робота з документами службового призначення на тему конфіденційної інформації в Секретаріату Кабінету Міністрів України	
12.09.2023 09:00-15:00	Оформлення висновку роботи з документами службового призначення на тему конфіденційної інформації в Секретаріату Кабінету Міністрів України	
13.09.2023 09:00-15:00	Огляд організації захисту інформації в структурних підрозділах.	
14.09.2023 09:00-15:00	Оформлення висновку результатів спостереження та сбіру інформації про автономні системи СКМУ	
15.09.2023 09:00-15:00	Робота з документами службового призначення на тему оптимізації роботи Секретаріату Кабінету Міністрів України в умовах воєнного стану	

Кінець додатка Б

16.09.2023 09:00-15:00	Аналіз технологічних систем захисту інформації в Секретаріаті Кабінету Міністрів України	
17.09.2023 09:00-15:00	Оформлення індивідуального завдання (Аналіз технологічних систем захисту інформації в Секретаріаті Кабінету Міністрів України)	
18.09.2023 09:00-15:00	Оформлення індивідуального завдання (Посадові інструкції про діяльність Секретаріату Кабінету Міністрів України в умовах особливого стану)	
19.09.2023 09:00-15:00	Праця з кваліфікаційною роботою. (Захист інформації в Секретаріаті КМУ)	
20.09.2023 09:00-15:00	Створенная презентації для захисту переддипломної практики.	
21.09.2023 09:00-15:00	Робота над помилками в оформленні звітної документації	
22.09.2023 09:00-15:00	Захист практики в аудиторному режимі	
23.09.2023	Робота з оформлення звітної документації	
24.09.2023	Завершення оформлення індивідуального завдання.	
25.09.2023	Здача звітної документації на кафедру	

Здобувач Ігор СЛЮСАР

Керівник від університету Ірина ТЮРМЕНКО

Керівник від бази практики Світлана КРИВИЛЕНКО