МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра управління імені Олега Балацького

«До захисту допущено»
Завідувач кафедри
_____ Ігор РЕКУНЕНКО
(підпис)
____ _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістра

зі спеціальності 281 «Публічне управління та адміністрування», освітньо-професійної програми «Адміністративний менеджмент»

на тему: Удосконалення управління системами інформаційної безпеки в державних органах влади регіонального рівня

Здобувача групи АМ.м - 31 Пугача Ігоря Олександровича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Ігор ПУГАЧ
(підпис)

Керівник Старший викладач, к. е. н., доцент,
Каріна ТАРАНЮК
_____
(підпис)

Суми – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра управління імені Олега Балацького

Завідувач кафедри
_____ Ігор РЕКУНЕНКО
(підпис)
____ _____ 2024р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр

зі спеціальності 281 «Публічне управління та адміністрування», освітньо-професійної програми «Адміністративний менеджмент»

Здобувача групи АМ.м - 31 Пугача Ігоря Олександровича

1. Тема роботи «Удосконалення управління системами інформаційної безпеки в державних органах влади регіонального рівня» затверджена наказом №1209-VI від 25.11.2024 р.
2. Термін подання здобувачем закінченої роботи 12.12.2024 р.
3. Мета кваліфікаційної роботи: дослідження пошук шляхів удосконалення процесів управління системами інформаційної безпеки в державних органах влади регіонального рівня
4. Об’єкт дослідження: процес управління системами інформаційної безпеки в державних органах влади регіонального рівня
5. Предмет дослідження: організаційно-правові відносини, які виникають в процесі функціонування систем інформаційної безпеки
6. Кваліфікаційна робота виконується на підставі_ статистичної звітності, періодичних видань, монографій, електронних ресурсів.
7. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети.

№ пор.	Назва розділу	Термін подання
I	Теоретичні аспекти інформаційної безпеки	24.11.2024
II	Методико-аналітична сутність управління інформаційною безпекою	30.11.2024
III	Удосконалення системи управління інформаційною безпекою в органах влади регіонального рівня	12.12.2024

Зміст завдань для виконання поставленої мети кваліфікаційної роботи:

У розділі 1 студент повинен дослідити теоретичні аспекти інформаційної безпеки, дослідити законодавчі та нормативні акти, виявити проблеми та виклики процесу цифрової трансформації.
У розділі 2 студент повинен проаналізувати сутність управління інформаційними системами, ІТ інфраструктурою та системами інформаційної безпеки в органах державної влади.
У розділі 3 студент повинен надати рекомендації щодо удосконалення системам управління інформаційною безпекою в органах державної влади регіонального рівня.

8. Консультації щодо виконання роботи:

Розділ	Прізвище, ініціали та посада керівника/консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Таранюк К.В., ст. викладач	18.11.2024	24.11.2024
2	Таранюк К.В., ст. викладач	24.11.2024	30.11.2024
3	Таранюк К.В., ст. викладач	30.11.2024	12.12.2024

9. Дата видачі завдання18.11.2024

Керівник кваліфікаційної роботи старший викладач, к. е. н., доцент, Каріна ТАРАНЮК _____
(підпис)

Завдання до виконання одержав Ігор ПУГАЧ _____
(підпис)

АНОТАЦІЯ

Структура та обсяг кваліфікаційної роботи. Загальний обсяг кваліфікаційної роботи магістра складає 58 сторінок, вступ, три розділи, десять підрозділів, висновки, додаток. Робота містить 2 таблиці, 7 рисунків, 54 використаних джерела.

Актуальність дослідження. Актуальність теми магістерської роботи полягає в тому, що недоліки в системі управління інформаційною безпекою можуть привести до негативних наслідків, особливо в умовах воєнного стану. Захист інформації та кібербезпека мають бути одним з пріоритетних напрямків діяльності в органах державної влади. Одним із пріоритетних напрямів покращення систем управління інформаційною безпекою є впровадження в органи державної влади регіонального рівня комплексних політик безпеки. Актуальність відзначається провідною роллю управлінських інновацій для забезпечення ефективності функціонування систем інформаційної безпеки.

Метою магістерської роботи є дослідження пошук шляхів удосконалення процесів управління системами інформаційної безпеки в державних органах влади регіонального рівня.

Методами дослідження магістерської роботи є систематизовані (евристичні, експертних оцінок, метод «мозкова атака»), системно-цільові (методи системного аналізу).

Об’єкт дослідження: процес управління системами інформаційної безпеки в державних органах влади регіонального рівня.

Предмет дослідження: організаційно-правові відносини, які виникають в процесі функціонування систем інформаційної безпеки.

Ключові слова: адміністрування, управлінські рішення, державне регулювання, інформаційна безпека, орган державної влади, політика безпеки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЄС – Європейський союз

ІБ – інформаційна безпека

ІзОД – інформація з обмеженим доступом

ІТС – інформаціно-телекомунікаційна система

КСЗІ – комплексна система захисту інформації

НД ТЗІ – нормативний документ технічного захисту інформації

ОДА – обласна державна адміністрація

СУІБ – система управління інформаційною безпекою

США – Сполучені штати Америки

ЦАЗІ – Центр антивірусного захисту інформації

ЦНАП – Центр надання адміністративних послуг

CCPA – California Consumer Privacy Act (Каліфорнійськи акт про захист приватності)

GDPR – General Data Protection Regulation (Загальний регламент захисту даних)

IoT – internet of things (інтернет речей)

NIST – National institute of standards and technology (Національний інститут стандартизації та технологій)

ВСТУП

Актуальність теми магістерської роботи полягає в тому, що недоліки в системі управління інформаційною безпекою можуть привести до негативних наслідків, особливо в умовах воєнного стану.

Об’єктом дослідження є процес управління системами інформаційної безпеки в державних органах влади регіонального рівня.

Предметом дослідження є організаційно-правові відносини, які виникають в процесі функціонування систем інформаційної безпеки.

До використаних методів дослідження належать: системний метод – при розвитку теоретичних положень дослідження; метод структурного аналізу – при аналізі законодавства; абстрактний метод – при встановленні рекомендацій; метод узагальнення – при формуванні загальних висновків дослідження.

Цифровий та інформаційний розвиток суспільства значно розширив можливості спілкування на відстані. Ведення бізнесу, фінансові операції, обмін інформацією стали швидкими й доступними завдяки мережі Інтернет. Цей стрімкий розвиток, окрім безперечних переваг, несе за собою й нові виклики, пов'язані з кібербезпекою. Підприємства стикаються з ризиком кібератак, крадіжок даних та інших загроз, а це може призвести до значних фінансових втрат та шкоді репутації. Водночас зростає проблема кіберзахисту об’єктів інформаційної інфраструктури, персональних даних осіб, які обробляються в інформаційно-комунікаційних системах, державної таємниці, іншої інформації з обмеженим доступом і вимагає посилення заходів для їх захисту від несанкціонованого доступу, використання та розкриття.

Беззаперечно можна стверджувати, що темпи розвитку законодавства, інших нормативних актів не завжди відповідають динаміці розвитку технологій, у свою чергу це призводить до проблем з правовим регулюванням кібервзаємовідносин, передусім в питаннях захисту персональних даних.

Забезпечення необхідного та достатнього рівня кіберзахисту в органах державної влади, особливо регіонального рівня, є важливим для забезпечення стійкості та обороноздатності регіону та держави в цілому.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Аналіз досліджень та публікацій

Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації та відповідно сформульованої національної інформаційної стратегії в значній мірі сприяла б забезпеченню досягнення успіху при вирішенні задач у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, запровадження вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. У сфері інформаційної безпеки знання (в будь-якій формі їх подання) виступають, з одного боку, як об'єкт безпосереднього захисту, а з другого – як фактор забезпечення інтересів людини, суспільства та країни у будь-якій сфері їх життєдіяльності на інформаційному рівні. Під методологічними засадами інформаційної безпеки розуміємо єдність концептуальних, теоретичних і технологічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності, а також сфер формування, обігу, накопичення і використання інформації. Предметом методології інформаційної безпеки є дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх запобіганню, своєчасному виявленню і нейтралізації.

Чіткого визначення поняття інформаційної безпеки або кібербезпеки в нинішньому законодавстві України не наведено, проте є визначення загального поняття «захист інформації».

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї (З-н Про інформацію, 1992).

Загальноприйнятими у світі та Україні критеріями (НД ТЗІ 2.5-004-99, 1999) для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступенів захищеності прийнято вважати:

1) Конфіденційність

Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги відносяться до критеріїв конфіденційності.

2) Цілісність

Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку, якщо існують вимоги щодо обмеження можливості модифікації інформації, то їх відносяться до критеріїв цілісності.

3) Доступність

Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то їх відносяться до критеріїв доступності.

Згідно з українським законодавством (Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки, 2007), розв'язання проблеми інформаційної безпеки має здійснюватися шляхом:

– створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;

– вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії

кіберзлочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Варто зазначити, що більшість законодавчих та нормативно-правових актів України є застарілими, та потребують актуалізації. Процес підтримки актуальності має бути неперервним, через стрімкий та постійний розвиток інформаційних технологій та систем передачі інформації.

Інформація беззаперечно потребує захисту в різних областях і, відповідно, дослідження проводяться в різних напрямках. Є роботи, в яких досліджуються кримінально-правове регулювання злочинів кібершахрайства з точки зору захисту персональної інформації громадян (Yu Zhang&Haoyun Dong, 2023). Інші вчені (Brown, Truby, Ibrahim, 2022) вивчають проблеми усунення прогалин в Загальному європейському регламенті захисту даних (General Data Protection Regulation, 2016). Є роботи, де аналізуються проблеми безпеки в соціальних мережах (Троценко, Снігуров, 2014). Досліджуються проблеми, які в пов’язані з використанням Інтернету речей (IoT) і захистом конфіденційності користувачів (Romansky, 2023). Також проводиться порівняння нормативних вимоги України та інших країн, які спрямовані на захист персональних даних (Кальченко, Ободяк, 2023; Кальченко, Ободяк, Пугач, 2024). Також розглядаються питання захисту об’єктів критичної інфраструктури (Puhach, Liubchak, 2024), розпочато аналіз нормативно-правового регулювання інформаційної безпеки в органах державної влади (Пугач, Таранюк, 2024).

Потрібно звернути увагу, що багато дослідників звертають увагу на захист конфіденційної інформації і не розглядають кіберзахист систем, де ця інформація знаходиться. Такий підхід може зашкодити персональним даним

при кібератаках. Але і безпосередній захист даних, і кіберзахист систем в цілому важливі для забезпечення надійного захисту даних.

1.2 Аналіз законодавства в сфері інформаційної безпеки

Відповідно до Закону України «Про інформацію» (1992) інформацією, що циркулює в системі органів державної влади, є відкрита та інформація з обмеженим доступом (ІзОД). До ІзОД відноситься таємна інформація (державна таємниця), інформація для службового користування та конфіденційна інформація (персональні дані фізичних осіб та конфіденційна інформація про юридичних осіб).

Найбільшого захисту в системі органів державної влади потребує державна таємниця, незалежно від грифу секретності. В цілому захист таємної інформації та державних інформаційних ресурсів регламентується Законом України «Про державну таємницю». Законом встановлено компетенції державних органів у сфері охорони державної таємниці, порядок надання допуску та доступу до цієї інформації. Уповноваженим органом щодо забезпечення захисту секретної інформації є Служба безпеки України.

Службова інформація або ж інформація для службового користування це «інформація що міститься в документах суб’єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень» (Про доступ до публічної інформації, 2023). Обмеження доступу до такої інформації може здійснюватися лише при наявності трьох вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для

запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Конфіденційна інформація в свою чергу поділяється персональні дані фізичних осіб та комерційні таємниці юридичних осіб. Основну увагу необхідно звернути саме на дані фізичних осіб, адже сюди включаються як дані звичайних громадян, так і державних службовців, витік яких може завдати значної шкоди особистій та професійній діяльності.

В статті 32 Конституції України (1996) зазначається «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Питання щодо персональних даних порушуються також у кількох інших нормативних актах:

1) Закон України «Про інформацію» (1992) – регулює відносини щодо одержання та поширення інформації.

2) Закон України «Про захист персональних даних» (2010) – визначає захист і обробку персональних даних .

3) Закон України «Про доступ до публічної інформації» (2011) – надає право на отримання інформації, що знаходиться у володінні розпорядників.

Зважаючи на значну захищеність таємної інформації, що знаходится у зоні відповідальності Служби безпеки України та Державної служби спеціального зв’язку та захисту інформації, та тимчасовість необхідного рівня захисту службової інформації, пріоритетним напрямком в системі управління інформаційною безпекою в органах державної влади регіонального рівня має бути саме захист персональних даних.

У відповідності до статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» (1994) «інформація, вимога щодо

захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. Підтвердження відповідності КСЗІ здійснюється за результатами державної експертизи в порядку, встановленому законодавством». В Україні є нормативні документи технічного захисту інформації (НД ТЗІ) в яких висуваються вимоги як до КСЗІ. На даний момент відсутні НД ТЗІ в яких чітко висуваються технічні вимоги щодо захисту персональних даних.

Основною проблемою в системі управління інформаційною безпекою як в органах державної влади так і на об’єктах критичної інфраструктури є відсутність чітко та однозначно визначених нормативних вимог, щодо функціонування інформаційних та інформаційно-комунікаційних систем, які використовуються в процесі діяльності.

Є «Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури» (2019), в яких містяться вимоги щодо кіберзахисту даних. Але цей документ регламентує порядок кіберзахисту тільки об'єктів критичної інформаційної інфраструктури, що внесені до відповідного переліку.

Нормативні документи України, які безпосередньо стосуються персональних даних (Про захист персональних даних, 2010; Типовий порядок обробки персональних даних, 2014) не містять чітких і явних вимог щодо кіберзахисту таких даних.

В «Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» (2006) є вимоги з кіберзахисту, які можна віднести і до захисту персональних даних:

– Захист цілісності інформації (пункти 5).

– Забезпечення криптографічного захисту (пункти 9, 13).

– Забезпечення реєстрації подій (пункт 11).

– Розмежування повноважень привілейованого та звичайного користувача (пункт 11).

– Забезпечення антивірусного захисту (пункт 16).

1.3 Аналіз іноземного законодавства в сфері інформаційної безпеки

У зв’язку з безупинним рухом України до ЄС та необхідністю приведення реформ у всіх галузях, включаючи захист інформації, необхідно звернути особливу увагу на норми, що діють в європейські зоні.

У відповідності до «Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони» (2017), а саме в пункті 11 цього плану є завдання «Удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679». 7 червня 2021 р. було подано проект Закону України «Про захист персональних даних» (2021), але він був відхилений. 25 жовтня 2022 р. подано новий проект цього Закону України (2022), який прийнятий у першому читанні Верховною Радою.

Положеннях GDPR (General Data Protection Regulation) є основою цього проекту. Вводиться, наприклад, посада “Відповідальна особа з питань захисту персональних даних”, вводяться штрафи за порушення законодавства про персональні дані. В ньому також пропонується внести зміни у положення інших нормативних актів, які торкаються обробки персональних даних.

Норми GDPR застосовуються на всі території ЄС, а також зазначається: «якщо персональні дані передаються з Союзу до контролерів, операторів або інших одержувачів у третіх країнах або до міжнародних організацій, рівень захисту фізичних осіб, який забезпечує в Союзі цей Регламент, не повинен бути ослабленим» (Регламент Європейського Парламенту і Ради, 2016).

Згідно цього регламенту персональними даними може бути будь-яка інформація щодо особи. Вказується виключний перелік підстав для опрацювання таких даних і права фізичної особи на доступ до цих даних і право на їх вилучення. Наводяться санкції за порушення регламенту, а також ситуації коли його не застосовують до опрацювання персональних даних.

GDPR застосовується в кожній з держав-членів ЄС без необхідності внесення його до законів цих країн. Однак він надає можливість в цих країнах вносити зміни в своє законодавство.

В Австрії (Federal Act concerning the Protection of Personal Data, 2019), наприклад, своїми персональними даними дитина розпоряджається з 14 років, а не з 16 в GDPR.

В Хорватії (Act on the implementation of the general data protection regulation, 2018) посилений захист персональних даних неповнолітніх.

В Чехії (Act about the processing of personal data, 2019), Данії (Databeskyttelsesloven, 2018), Франції (La loi Informatique et Libertés, 2015), Німеччині (Federal Data Protection Act, 2021), Ірландії (Data protection act, 2018), Італії (Personal data protection code, 2019), Нідерландах (Uitvoeringswet Algemene verordening gegevensbescherming, 2021), Польщі (The Act of 10 May 2018 on the Protection of Personal Data, 2018), Іспанії (Ley Orgánica de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, 2018), Швеції (Lag med kompletterande bestämmelser till, 2018) приділено увагу роботі з персональними даними в бізнесі.

В Фінляндії (Data Protection Act, 2018) дитина може з 13 років розпоряджатися своїми персональними даними замість 16 років в GDPR. В цій країні встановлено жорсткий максимальний термін для повідомлення про витік даних - 24 години (в GDPR -72 години).

В Литві (Republic of Lithuania Law on legal protection of personal data, 2016) своїми персональними даними дитина розпоряджається з 14 років, а не з 16 в GDPR.

GDPR – це основний регуляторний документ ЄС стосовно персональних даних. Він надає всім зацікавленим сторонам більше контролю над їхніми даними та вимагає від організацій дотримуватися строгих процедур захисту даних. Але є і інші документи в ЄС про персональних дані (Mantelero et al., 2020), дія яких розповсюджується на всі країни-учасники ЕС:

Директива 2015/2366 щодо платіжних сервісів та послуг (Directive (EU) 2015/2366, 2015) – це директива ЄС, яка регулює платіжні послуги та платіжних посередників з метою збільшення конкуренції та підвищення безпеки платежів у ЄС.

Регламент 910/2014 «Щодо електронної ідентифікації та довірчих послуг» (Regulation (EU) No 910/2014, 2014) – це регламент встановлює правила для електронних ідентифікацій та довірчих послуг для електронних транзакцій в ЄС.

Директива 2022/2555, щодо підвищення рівня кіберзахищеності (. Directive (EU) 2022/2555, 2022) – це директива ЄС, яка спрямована на забезпечення вищого рівня кібербезпеки в усіх країнах-членах, розширюючи обов'язки та вимоги до різних секторів та послуг.

Враховуючи накладені санкції за порушення GDPR, які досягають сотень мільйонів євро, цей регламент можна вважати дієвим механізмом для збереження персональних даних. В цьому регламенті не вказано, яким чином створювати інформаційно-комунікаційні системи, які повинні забезпечувати дотримання його положень.

Не варто оминати увагою регулювання у Сполучених штатах Америки, які є лідером та одним із основних гравіців у сфері кібербезпеки та захисту інформації у світі.

В США діє Закон «Про приватність» (The Privacy Act, 1974), ухвалений у 1974 році. В цьому законі закладені основи захисту персональних даних. Але оскільки він прийнятий пів століття тому назад, то принципи захисту персональних даних в ньому далекі від сучасного стану інформаційних систем, а нового федерального закону США не ухвалено.

З 1 січня 2020 р. в Каліфорнії діє закон про захист персональних даних споживачів (California Consumer Privacy Act, 2018). Цей закон вносить зміни в розділ «Персональні дані» цивільного кодексу Каліфорнії (The Civil Code of California, 1872). В цьому законі зазначено, що той про кого збираються такі дані, має знати для чого збирається інформація і які ці дані. Також при

перевіреному запиті споживача, розпорядник інформації повинен видалити персональну інформацію цієї особи.

Особливістю визначення терміну «персональні дані» в CCPA є те, що крім особистої інформації, яка ідентифікує особу, така інформація може стосуватись і домогосподарства.

Окрім законів в США діє стандарт NIST Privacy Framework (2020). Його положення про захист персональних даних подібні до положень CCPA та GDPR .

Стандарт є добровільним документом, тобто кожна організація використовує його для того, щоб забезпечити збереження персональних даних, включаючи ризики конфіденційності IoT чи штучного інтелекту.

До особливостей цього стандарту можна віднести покроковість його впровадження. Почати потрібно з оцінки ризиків конфіденційності, а потім розробляти персоналізовані програми конфіденційності. На кінцевому етапі включаються процеси захисту персональних даних.

Згідно цього стандарту необхідно постійно контролювати діяльність і, при необхідності, вносити зміни.

1.4 Особливості процесів цифрової трансформації

Цифрова трансформація є невід'ємною частиною сучасного розвитку будь-якої країни, в тому числі й України. Вона відкриває безліч можливостей для економічного зростання, поліпшення якості життя та підвищення конкурентоспроможності. Однак, як і будь-який масштабний процес, цифрова трансформація пов'язана з певними ризиками та проблемами.

Перше про що варто зазначити – це «цифрова нерівність». Обмежений та нерівномірний доступ до інтернету та цифрових технологій у різних регіонах України значною мірою уповільнюють темпи цифровізації. Відсутність або недостатність цифрових навичок населення, яке володіє цифровими навичками для ефективного використання нових технологій, що в свою чергу призводить

до соціального розшарування та поглиблення соціальної нерівності через відсутність доступу до цифрових послуг.

Наступним недоліком можна виділити залежність від іноземних технологій. Останніми роками технологічна залежність України дещо знизилась у зв’язку з появою вітчизняних розробників програмного забезпечення та власне програмних засобів, як державних так і комерційних. Однак ризик від надмірної залежності від іноземного обладнання залишається через відсутність матеріально-технічної бази для розвитку високотехнологічних виробництв, особливо в нинішніх умовах. Також існує загроза для функціонування критичної інфраструктури, яка залежить від іноземних технологій, таких як серверне, комунікаційне та контрольне обладнання.

Іншим викликом є зміна ринку праці. У зв’язку з автоматизацією робочих місць зростають вимоги, щодо цифрових навичок нових співробітників, а також зростає ризик втрати робочих місць через автоматизацію окремих процесів. До цієї категорії також можна віднести необхідність проведення додаткових навчань, курсів та тренувань для підвищення рівня цифрової обізнаності наявного персоналу.

Також однією з найзначніших проблем є безпека, як технічних та програмних засобів так і особистості. В процесі цифровізації зростає кількість пристроїв, підключених до мереж будь-якого рівня, що значно збільшує кількість векторів можливих атак на пристрої та систему в цілому. Модернізація ІТ-інфраструктури, яка є необхідною, часто призводить до ускладнення та перевантаження, що ускладнює виявлення та усунення вразливостей відповідальними особами.

Недостатнє фінансування заходів з кібербезпеки та значний дефіцит кваліфікованих кадрів в державному секторі обмежує можливості для впровадження сучасних засобів та технологій захисту. Однак варто визначити, що удосконалення систем захисту не забезпечить безпеки, адже кіберзлочинці постійно вдосконалюють свої методи, використовуючи нові технології, соціальну інженерію та інші методи для досягнення бажаного результату.

Також проблемою в процесі забезпечення кібербезпеки є використання обладнання, що забезпечує захист, адже зазвичай використовуються засоби іноземних виробників. В цьому випадку варто згадати випадок з камерами відеоспостереження відомих та розповсюджених у світі виробників. Камери мали в собі вразливість та дозволяли підключення з віддалених пристроїв, а також програмне забезпечення для відеоспостереження, що було доступне ворожими розвідкам (Овсяний, 2023).

Також важливою проблемою є захист персональних даних та порушення права на приватність через збір та використання особистих даних, що в свою чергу, в разі витоку відкриває можливості до проведення інших злочинних дій.

До найрозповсюдженіших злочинних дій, можна віднести:

1) Фішинг та соціальна інженерія: Зловмисники використовують різноманітні методи обману для отримання доступу до конфіденційної інформації.

2) Вразливості програмного забезпечення: Незаплановані уразливості в програмному забезпеченні можуть бути використані для проникнення в системи.

3) DOS/DDoS-атаки: атаки відмови в обслуговуванні можуть вивести з ладу важливі ресурси.

4) Викрадення даних: Зловмисники можуть викрадати конфіденційні дані для їх подальшого використання в злочинних цілях.

5) Втручання в роботу критичної інфраструктури: Кібератаки можуть призвести до збоїв у роботі енергетичних систем, транспортних мереж та інших критично важливих об'єктів.

6) Маніпуляція громадською думкою: Використання цифрових технологій для поширення дезінформації та маніпуляцій.

Аналізуючи показники індексу цифрової трансформації регіонів України (рис. 1.1) за 2023 рік (Міністерство цифрової трансформації, 2024), можна побачити що узагальнений показник для Сумської області 0.178 та є останнім,

не враховуючи тимчасово окуповані території. Значення показиників наведені в таблиці А.1.

Індекс формується за результатами діяльності галузевих заступників голів обласних адміністрацій та складається з восьми субіндексів, які характеризують окремі складові частини процесу цифровізації:

1) Інституційна спроможність (наявність підрозділу цифровізації, наявність стратегії та програми інформатизації).

2) Розвиток інтернету (підключення укриттів та закладів до інтернету, доступ до нфраструктури).

3) Розвиток ЦНАП (кількість, якість та автоматизація послуг, безбар'єрність).

4) Впровадження режиму «без паперів» (електронний документообіг, оцифрування реєстрів).

5) Цифрова освіта (освітні інформаційні системи в закладах освіти).

6) Візитівка області (вебсайт ОДА, геоінформаційні системи).

7) Проникнення базових е-послуг (цифровізація соціальної сфери).

8) Галузева цифрова трансформація (захист інформації, політика кібербезпеки, охорона здоров'я, цивільний захист).

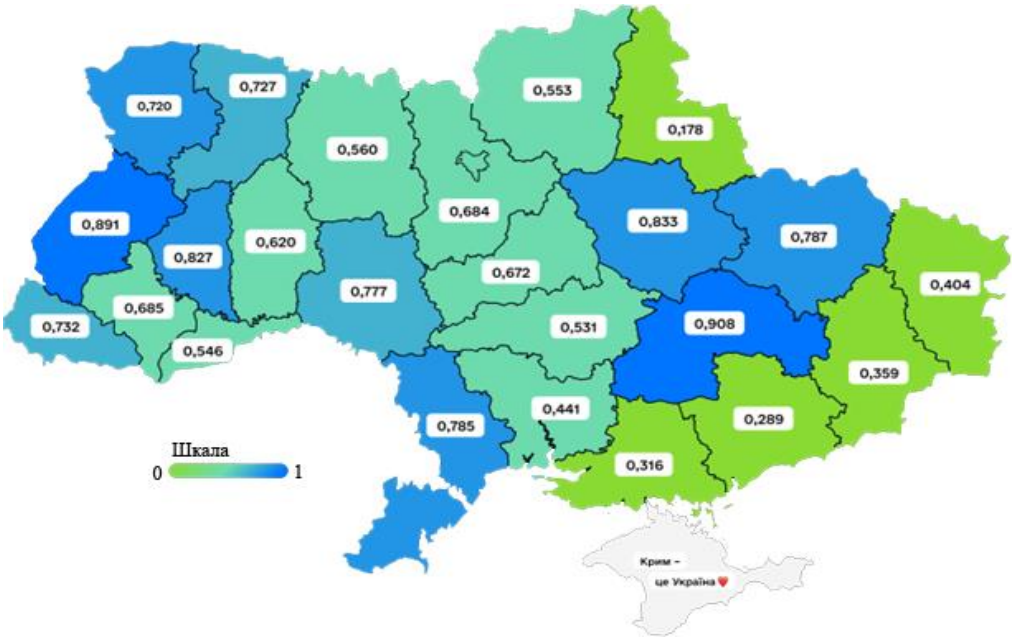

Рисунок 1.1 – Узагальнені показники індексу цифрової трансформації регіонів

Джерело: Міністерство цифрової трансформації, 2024

Значення субіндексів наведено в таблиці А.2. В рамках роботи розглянемо показник галузевої цифрової трансформації Сумської області, який складає 0.104, що може вказувати на критично низький рівень забезпечення кібербезпеки і відсутність політики інформаційної безпеки в органах влади та комунальних закладах регіону, а також на відсутність інструментів електронної демократії.

РОЗДІЛ 2. МЕТОДИКО-АНАЛІТИЧНА СУТНІСТЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Принципи управління IT системами

Управління IT системами – це процес, яка охоплює широкий спектр процесів, спрямованих на ефективне використання інформаційних технологій в організації. Дотримання певних принципів дозволяє забезпечити безперебійну роботу систем, підвищити їхню продуктивність та безпеку, а також сприяти досягненню стратегічних цілей.

До основних принципів управління IT інфраструктурою можна віднести:

1) Планування та стратегія:
   a) Визначення цілей – чітко визначити цілі та завдання, які має вирішувати IT система.
   b) Стратегічне планування – розробити стратегію розвитку IT системи, враховуючи потреби та майбутні тенденції.
   c) Бюджетування – Забезпечити фінансове планування та контроль над витратами на IT.
2) Безпека та конфіденційність:
   a) Захист даних – забезпечити надійний захист даних від несанкціонованого доступу, модифікації або знищення.
   b) Управління ризиками – визначити та оцінити потенційні ризики, пов'язані з IT системою, та розробити заходи для їх мінімізації.
   c) Створення резервних копій –регулярно створювати резервні копії даних та програмного забезпечення для відновлення в разі аварії.
3) Ефективність та продуктивність:
   a) Оптимізація ресурсів – забезпечити раціональне використання обчислювальних ресурсів, мережі та програмного забезпечення.

b) Моніторинг та аналіз – регулярно моніторити роботу IT системи та аналізувати її ефективність.
c) Автоматизація – використовувати автоматизацію для спрощення рутинних завдань та підвищення продуктивності.

4) Зручність використання та доступність:
   a) Інтуїтивний інтерфейс – забезпечити зручний та інтуїтивний інтерфейс для користувачів.
   b) Надійність та доступність – забезпечити безперебійну роботу IT системи та доступність до необхідних ресурсів.
   c) Підтримка користувачів – надати користувачам необхідну допомогу та підтримку.
5) Сумісність та інтеграція:
   a) Всі IT-системи повинні працювати як єдине ціле, забезпечуючи безперебійний обмін даними та інформацією.
   b) Сумісність з іншими системами – забезпечити сумісність IT системи з іншими системами та програмним забезпеченням.
   c) Інтеграція з бізнес-процесами – інтегрувати IT систему з бізнес-процесами для підвищення ефективності та продуктивності.
6) Оновлення та розвиток:
   a) Регулярні оновлення – регулярно оновлювати програмне забезпечення та операційні системи для забезпечення безпеки та стабільності.
   b) Впровадження нових технологій – впроваджувати нові технології та інновації для покращення роботи IT системи.
   c) Модернізація – регулярно модернізувати IT систему для відповідності сучасним вимогам та потребам.
7) Управління змінами:
   a) Планування та контроль – впроваджувати зміни в IT системі за планом, контролюючи їх вплив.
   b) Тестування та документування – тестувати зміни перед їх впровадженням та документувати процес внесення змін.

c) Зворотний зв'язок – збирати та аналізувати зворотний зв'язок від користувачів для покращення роботи IT системи.

Ці принципи є основними для ефективного управління IT системами та забезпечення їх надійної роботи, однак перелік не є виключним та залежить від складності системи та необхідності постійних змін та модернізацій в конфігурації систем пов’язаних із технічним розвитком

Для ефективного управління IT-системами широко використовуються різноманітні стандарти, такі як:

– Бібліотека інфраструктури інформаційних технологій (ITIL): Набір найкращих практик для управління IT-послугами.

– Цілі контролю для інформаційних та суміжних технологій (COBIT) –фреймворк для оцінки та покращення управління IT-інфраструктурою та суміжними процесами.

– ISO/IEC 27001 (2022): Міжнародний стандарт з кібербезпеки та управління інформаційною безпекою.

2.2 Система управління інформаційною безпекою

Система управління інформаційною безпекою (СУІБ,ISMS) – це комплекс заходів, спрямований на захист інформації протягом усього її життєвого циклу. Метою системи управління інформаційною безпекою (СУІБ) є мінімізація ризиків, пов'язаних з інформацією, та забезпечення безперебійної роботи бізнес-процесів.

Управління ІБ може бути представлено як циклічний та періодичний процес (рис. 2.1), який можна представити циклом PDCA (плануй-виконуй-перевіряй-дій, *Plan-Do-Check-Act*):

– Plan (планування) – проектування СУІБ, розробка переліку активів, оцінка ризиків та підбір заходів;

– Do (дія) – створення та введення в експлуатацію запланованих заходів;

– Check (перевірка) – оцінка результативності СУІБ за результатами

проведення аудиту;

– Act (удосконалення) – коригування та зміна параметрів системи.

Рисунок 2.1 – Процес управління інформаційною безпекою

Джерело: створено автором

Побудова СУІБ дозволяє створити детальну картину взаємодії процесів та підсистем інформаційної безпеки, визначити ролі та обов’язки персоналу, а також оцінити необхідні фінансові та людські ресурси для ефективного функціонування системи.

До основних функцій системи управління інформаційною безпекою:

– виявлення та аналіз ризиків;

– планування та реалізація процесів, для мінімізації ризиків ІБ;

– контроль цих процесів;

– внесення в процеси мінімізації ризиків необхідних коригувань.

Якісне управління інформаційною безпекою передбачає:

– Всеосяжний підхід: охоплення всіх компонентів інформаційної системи та врахування всіх внутрішніх та зовнішніх загроз.

– Інтеграцію з бізнесом: узгодження заходів ІБ з бізнес-цілями та стратегією підприємства.

– Високий рівень контролю: можливість ефективно керувати процесами інформаційної безпеки.

– Використання актуальною інформації: застосування даних, які відповідають потребам системи.

– Оптимізацію ресурсів: досягнення максимальної ефективності за мінімальних витрат.

– Постійне вдосконалення: пошук нових рішень та адаптацію до змінних умов.

– Системний підхід: використання циклічного процесу планування, виконання, контролю та вдосконалення.

Міжнародна європейська агенція з кібербезпеки розробила рамку ISMS (The ISMS Framework, 2022) , яка є європейським аналогом української СУІБ. Ця рамка пропонує детальну схему для управління інформаційною безпекою, яке відбувається за схемою, відображеною на рисунку 2.1.

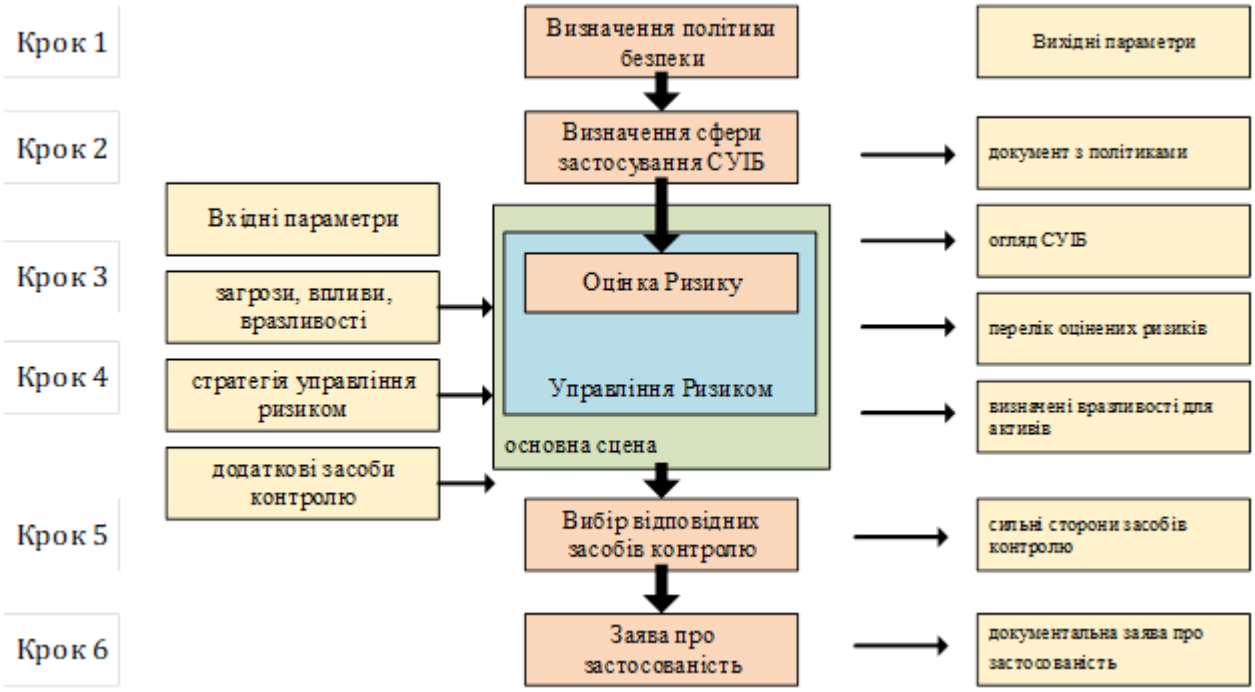

Рисунок 2.1 – СУІБ відповідно до фреймворку ISMS від ENISA

Джерело: створено автором за данимим ENISA

І розмір організації чи установи, й конкретний вид діяльності диктує вимоги безпеки, на правовому, регуляторному та операційному рівнях.

Малі установи без вимог до обробки персональних даних часто інтегрують питання інформаційної безпеки в загальний процес управління ризиками, не виділяючи їх в окрему систему.

Великі організації а також установи, такі як банки, телекомунікаційні компанії, лікарні та державні установи, стикаються з високими ризиками порушення інформаційної безпеки через обсяг та чутливість даних, якими вони володіють. Строгі законодавчі вимоги щодо захисту персональних даних, а також відповідальність за збереження конфіденційності клієнтів та громадян змушують їх приділяти особливу увагу інформаційній безпеці.

Враховуючи складність сучасних загроз та вимоги законодавства, розробка та впровадження систематизованого підходу до управління інформаційною безпекою, такого як Система управління інформаційною безпекою (СУІБ), є не просто бажаним, а й необхідним кроком для забезпечення захисту конфіденційних даних та бізнес-процесів.

Як показано на рисунку 2.1 , розробка СУІБ передбачає шість кроків:

1) визначення політики безпеки;
2) визначення сфери застосування СУІБ;
3) оцінка ризику (як частина управління ризиками);
4) управління ризиками;
5) вибір відповідних засобів контролю;
6) заява про застосовність.

Етапи 3 та 4 процесу оцінки та управління ризиками в СУІБ виконують роль своєрідного каталізатора, який перетворює абстрактні концепції інформаційної безпеки у конкретні дії. З одного боку, вони беруть за основу загальні принципи, правила та цілі, закладені в політиці безпеки. З іншого боку, ці етапи деталізують ці цілі, перетворюючи їх у конкретні заходи контролю та механізми захисту. Таким чином, відбувається плавний перехід від стратегічного планування до тактичної реалізації заходів, спрямованих на мінімізацію ризиків та захист інформаційних активів організації.

Кроки 5 та 6 є суто операційними і стосуються практичного виконання заходів, визначених на попередніх етапах. Вони включають в себе технічну конфігурацію систем, налаштування програмного забезпечення, проведення тестів та моніторинг ефективності захисних заходів. Таким чином, ці кроки

забезпечують безперебійну роботу систем безпеки та їх відповідність вимогам, встановленим на етапі оцінки ризиків.

Для забезпечення інформаційної безпеки організації можуть використовувати широкий спектр засобів контролю. Ці засоби часто вибираються з переліку рекомендованих контролів, наведених у міжнародних стандартах, таких як ISO/IEC 27002 (2022). Однак, жодний стандарт не може повністю охопити всі можливі сценарії та вимоги. Тому, організації зазвичай адаптують та доповнюють загальні контролі, враховуючи специфіку своєї діяльності, розмір, структуру та рівень ризику. Такий індивідуальний підхід дозволяє створити більш ефективну систему захисту інформації.

Крок 6 передбачає створення деталізованого документа, в якому чітко відображаються всі виявлені ризики, що стосуються конкретної організації. Цей документ повинен містити не тільки опис ризиків, але й оцінку їхньої ймовірності та потенційних наслідків. На основі цієї оцінки організація вибирає оптимальні технічні засоби захисту та розробляє план їх впровадження. Цей план детально описує, як саме обрані механізми безпеки будуть інтегровані в існуючу IT-інфраструктуру організації.

Впровадження та підтримка СУІБ у великих організаціях передбачає циклічний процес, де етапи «визначення політики безпеки» та «визначення сфери застосування СУІБ» мають стратегічний характер і вимагають залучення вищого керівництва. Ці рішення приймаються нечасто і на тривалий період. Натомість, наступні етапи є більш операційними і виконуються регулярно, оскільки ризики інформаційної безпеки постійно змінюються.

Побудова системи управління інформаційною безпекою на основі міжнародного стандарту ISO/IEC 27001 є стратегічно важливим рішенням. Цей стандарт не лише забезпечує систематичний підхід до управління інформаційними ризиками, а й сприяє підвищенню рівня довіри громадян, партнерів та регуляторних органів. Дотримання вимог ISO/IEC 27001 демонструє, що організація серйозно ставиться до захисту своїх даних та готова забезпечити їх конфіденційність, цілісність та доступність.

ISO 27001 - це міжнародно визнаний стандарт, який надає організаціям структурований підхід до управління інформаційною безпекою. Він допомагає ідентифікувати, оцінювати та обробляти ризики, пов’язані з конфіденційністю, цілісністю та доступністю інформації. Стандарт пропонує детальні рекомендації щодо створення та підтримки системи управління інформаційною безпекою, включаючи розробку політик, процедур, призначення відповідальних осіб та проведення регулярних аудитів. Застосування ISO 27001 дозволяє організаціям демонструвати свій високий рівень відповідальності за захист інформації та довіри клієнтів.

Система управління інформаційною безпекою (СУІБ) не лише забезпечує вибір оптимальних методів захисту інформації, але й підвищує довіру до організації з боку клієнтів, партнерів та регуляторних органів. Варто зазначити, що СУІБ є гнучким інструментом, який дозволяє адаптуватися до специфічних потреб кожної організації.

Сьогодні існує широкий спектр стандартів, методик та інших документів, що регламентують управління інформаційною безпекою. Серед них можна виділити ISM3, COBIT, ITIL/ITSM, BSI-100-2, ISO13335-4, CRAMM та інші. Кожен з цих стандартів має свої особливості та фокусується на різних аспектах інформаційної безпеки. Однак, незважаючи на різноманітність, більшість з них є сумісними з міжнародним стандартом ISO 27001, який вважається одним з найпопулярніших та найавторитетніших у цій галузі. ISO 27001 встановлює вимоги до системи управління інформаційною безпекою та забезпечує основу для побудови ефективної та надійної захисту інформації в організації.

2.3 Система забезпечення інформаційної безпеки в органах державної влади

Державна політика національної безпеки в інформаційній сфері – це комплекс заходів, спрямованих на створення сприятливого середовища для розвитку інформаційного суспільства, забезпечення інформаційної безпеки

держави та захисту прав і свобод громадян у цифровому просторі. Ця політика має на меті:

– Гарантування конституційних прав: забезпечення вільного доступу до інформації та її використання для особистого розвитку та участі в суспільному житті.

– Формування національного інформаційного простору: створення єдиного інформаційного простору держави, що відповідає національним інтересам та культурним цінностям.

– Інтеграція у світовий інформаційний простір: активна участь у глобальних інформаційних процесах на засадах рівноправності та взаємовигідного співробітництва.

– Забезпечення інформаційної безпеки: захист інформаційної інфраструктури від зовнішніх загроз, запобігання кіберзлочинам та інформаційним війнам.

– Розвиток інформаційної індустрії: створення сприятливих умов для розвитку IT-сектору, підтримка інновацій та впровадження нових технологій.

– Формування інформаційної культури: підвищення рівня інформаційної грамотності населення, розвиток критичного мислення та медіаграмотності.

Система забезпечення інформаційної безпеки України – це розгалужена мережа взаємопов’язаних суб’єктів, кожен з яких відіграє важливу роль у загальній системі захисту інформаційного простору. Державні органи розробляють стратегію та нормативно-правову базу, спеціалізовані служби забезпечують технічний захист інформації, бізнес-структури впроваджують системи захисту інформації у своїх організаціях, а громадські організації та окремі громадяни підвищують рівень кібергігієни та сприяють формуванню інформаційної культури в суспільстві.

Основними напрямами системи забезпечення інформаційної діяльності держави є:

– Будівництво та розвиток стійкої інфраструктури інформаційної безпеки.

– Координація зусиль усіх учасників інформаційного процесу.

– Захист критичної інфраструктури.

– Впровадження інноваційних технологій захисту інформації.

– Міжнародне співробітництво.

– Аналіз загроз та інцидентів.

Основними суб’єктами системи забезпечення інформаційної безпеки України є:

– громадяни України;

– Верховна Рада України;

– Президент України;

– Рада Національної безпеки і оборони України;

– Кабінет Міністрів України;

– Національна комісія з питань регулювання зв’язку України;

– Служба безпеки України;

– Державна служба спеціального зв’язку та захисту інформації України;

– Міністерство внутрішніх справ України;

– Національна Рада України з питань телебачення та радіомовлення;

– Конституційний Суд України;

– суди загальної юрисдикції;

– Генеральна прокуратура України;

– органи місцевого самоврядування;

– інші державні органи та організації;

– засоби масової інформації;

– громадські організації та професійні спілки;

– неурядові дослідницькі організації;

– організації та установи, що здійснюють діяльність в інформаційній сфері.

В Україні створена система забезпечення інформаційної безпеки, яка охоплює широкий спектр заходів, спрямованих на захист державних інтересів у інформаційній сфері. Ця система базується на чітко визначених функціях та повноваженнях державних органів, які закріплені у відповідних нормативно-

правових актах. Однак, незважаючи на наявність законодавчої бази, система потребує подальшого вдосконалення, зокрема у частині розподілу функцій між різними суб'єктами та оптимізації механізмів їх взаємодії.

Інформаційна безпека є фундаментальним елементом сучасного суспільства, де інформація стала одним з найцінніших ресурсів. Її розвиток не обмежується лише технічним прогресом та розширенням можливостей обміну даними. Справжня інформаційна безпека передбачає комплексне та системне вирішення широкого кола питань, що виходять за рамки технологічних аспектів. Важливим аспектом є усвідомлення усіма учасниками інформаційних процесів – від окремих громадян до великих корпорацій та державних органів – необхідності забезпечення захисту інформації. Це означає не лише розуміння потенційних загроз, але й готовність вживати активних заходів для їх запобігання. Створення безпечного інформаційного простору потребує спільних зусиль з боку всіх зацікавлених сторін. Власники інформації повинні забезпечувати конфіденційність та цілісність своїх даних, користувачі – відповідально ставитися до інформації, яку вони отримують та передають, виробники інформаційних технологій – розробляти безпечні продукти та послуги, постачальники послуг – гарантувати надійність своїх систем, а держава – створювати сприятливе правове поле та координувати зусилля всіх учасників.

Актуальність вирішення проблеми захисту інформаційних ресурсів у сучасному світі зумовлена низкою чинників, які створюють значні загрози для інформаційної безпеки. Зростання цифрової залежності суспільства, поширення мережевих технологій та глобалізація інформаційних потоків суттєво розширили можливості для здійснення кібератак та інших видів інформаційного впливу.

Одним із ключових факторів, що посилюють актуальність цього питання, є значне збільшення кількості користувачів мережі Інтернет та інших інформаційних систем. Це створює сприятливі умови для діяльності кіберзлочинців, які прагнуть отримати несанкціонований доступ до

інформаційних ресурсів з метою їх крадіжки, модифікації або знищення. Зростання кількості користувачів також призводить до збільшення кількості вразливостей в інформаційних системах, що можуть бути використані злочинцями для реалізації своїх злочинних намірів.

Важливу роль у зростанні загроз інформаційній безпеці відіграє розвиток нових технологій. З одного боку, нові технології відкривають широкі можливості для розвитку суспільства та економіки. З іншого боку, вони створюють нові вектори для кібератак. Зокрема, поява таких технологій, як штучний інтелект, машинне навчання та блокчейн, дозволяє кіберзлочинцям розробляти більш складні та ефективні засоби атак.

Крім того, зростає загроза державно-спонсорованих кібератак, які спрямовані на дестабілізацію суспільства, підрив економіки та здійснення політичного шантажу. Такі атаки можуть мати далекосяжні наслідки і завдавати значної шкоди національній безпеці.

Особливо вразливими до кібератак є критична інфраструктура, системи управління виробництвом, енергетичні системи, транспортні системи та інші об'єкти, від яких залежить життєдіяльність суспільства. Порушення роботи таких систем може призвести до серйозних наслідків, включаючи фінансові втрати, соціальні потрясіння та навіть загрозу життю людей.

Наявність великих обсягів конфіденційної інформації в державних органах, банківських установах та інших критично важливих інфраструктурах вимагає впровадження надійних систем захисту. Сучасні кіберзагрози постійно еволюціонують, що ускладнює завдання забезпечення інформаційної безпеки. Тому необхідний комплексний підхід, який включає не лише технічні засоби захисту, а й організаційні заходи, підвищення обізнаності персоналу та регулярне оновлення нормативно-правової бази.

Захист інформації в Україні розгядається як комплекс взаємопов’язаних заходів правового, організаційного, технічного та іншого характеру, спрямованих на забезпечення безпеки інформаційного простору держави. Цей

процес охоплює не лише інформацію з обмеженим доступом, а й відкриті дані, які згідно з чинним законодавством потребують захисту.

Основною метою захисту інформації є забезпечення її цілісності, конфіденційності та доступності. Це означає, що інформація має зберігати свою структуру та зміст, не підлягати несанкціонованому доступу та бути доступною уповноваженим користувачам у необхідний момент часу.

Забезпечення інформаційної безпеки державних органів є складним завданням, яке вимагає комплексного підходу. Для ефективного захисту інформаційних ресурсів від різноманітних загроз, у тому числі трансграничних, необхідне поєднання юридичних, організаційних, технічних та інженерних заходів. Саме такий комплексний підхід дозволяє створити надійний захист інформаційних систем і даних.

Одним з ключових елементів цього процесу є розвиток правової бази. Сучасні реалії вимагають постійного вдосконалення законодавства в галузі інформаційної безпеки, з метою адаптації його до нових технологій та зростаючих загроз. Правові норми повинні не лише регулювати відносини в сфері захисту інформації, а й забезпечувати гармонізацію національного законодавства з міжнародними стандартами. Це дозволить Україні повноцінно брати участь у глобальному інформаційному обміні, зберігаючи при цьому свій інформаційний суверенітет.

Таким чином, створення ефективної системи забезпечення інформаційної безпеки державних органів є багатогранним процесом, який потребує системного підходу та постійного вдосконалення. Правова складова цього процесу відіграє визначальну роль, оскільки саме законодавство створює необхідні умови для забезпечення інформаційної безпеки на державному рівні.

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах охоплює комплекс заходів, спрямованих на забезпечення безпеки державних даних. Цей процес включає в себе формування загальної стратегії захисту, розробку нормативно-

правової бази, визначення критеріїв оцінки захищеності та безпосереднє виконання функцій уповноваженого органу в цій сфері.

Ключовими аспектами реалізації цієї політики є:

– Стратегічне планування: Розробка довгострокових планів розвитку системи захисту державних інформаційних ресурсів, визначення пріоритетних напрямів діяльності та розподіл ресурсів.

– Нормативно-правове забезпечення: Створення чітких правил і вимог до захисту інформації, які відповідають сучасним загрозам та викликам.

– Оцінка захищеності: Регулярний аналіз стану захищеності інформаційних систем для виявлення вразливостей та розробки заходів щодо їх усунення.

– Контроль та нагляд: Моніторинг дотримання встановлених вимог до захисту інформації та вжиття заходів у разі виявлення порушень.

– Міжнародне співробітництво: Співпраця з іншими країнами для обміну досвідом та розробки спільних підходів до захисту інформації.

Таким чином, реалізація державної політики в цій сфері є комплексним процесом, який вимагає скоординованих дій різних органів державної влади та суб’єктів інформаційних відносин.

Реалізація державної політики в галузі інформаційної безпеки передбачає комплекс заходів, спрямованих на захист державних інформаційних ресурсів. Зокрема, це стосується:

– Методичного керівництва та координації: розробки єдиних підходів та стандартів у сфері інформаційної безпеки, надання методичних рекомендацій органам державної влади, місцевого самоврядування та підприємствам.

– Збору та аналізу інформації: систематичного збирання даних про кібератаки та інциденти, проведення аналізу для виявлення трендів та вразливостей.

– Оцінки рівня захищеності: проведення регулярних оцінок стану захищеності інформаційних систем, виявлення слабких місць та розробки заходів для їх усунення.

– Реагування на інциденти: розробки планів реагування на кіберінциденти

та їх ефективної реалізації.

На сьогоднішній день підключення органів державної влади до мережі Інтернет здійснюється через захищені вузли Інтернет-доступу, які забезпечують фільтрацію трафіку, захист від кібератак та контроль за доступом до інформаційних ресурсів. Одним з ключових провайдерів таких послуг в Україні є Державна служба спеціального зв'язку та захисту інформації України. Перехід на використання захищених вузлів Інтернет-доступу Національної системи конфіденційного зв’язку є важливим кроком у напрямку підвищення рівня кібербезпеки держави. Це дозволить забезпечити надійний захист державної інформації, підвищити ефективність роботи державних органів та створити умови для розвитку цифрової економіки.

На виконання завдань Національної програми інформатизації у межах виконання проекту «Забезпечити антивірусний захист державних інформаційних ресурсів» створено Центр антивірусного захисту інформації (ЦАЗІ) (Про затвердження Порядку оновлення антивірусних програмних засобів, 2023). Одним із основних завдань ЦАЗІ є впровадження єдиної технологічної політики щодо антивірусного захисту інформації в ІТС органів державної влади, а також централізованого забезпечення їх антивірусними програмними продуктами, сертифікованими у встановленому законодавством України порядку.

Одним із важливих напрямків діяльності ЦАЗІ є проведення експертиз антивірусних програм. Ці експертизи дозволяють визначити, чи відповідають антивіруси українським стандартам безпеки та чи можуть ефективно захистити інформацію від кіберзагроз. Крім того, ЦАЗІ проводить експрес-експертизи оновлень до антивірусних програм, для забезпечення їх актуальності.

Для моніторингу стану захищеності інформації в державних інформаційних системах постановою Кабінету Міністрів України від 03.08.2005 № 688 затверджено Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади. У цей Реєстр включаються всі державні установи та організації, які працюють з

інформацією. Забезпечення функціонування цього Реєстру покладено на Департамент безпеки інформаційно-телекомунікаційних систем, який здійснює регулярний контроль за рівнем захищеності інформації в цих організаціях.

Для ефективного протистояння загрозам інформаційній безпеці держави необхідно систематично проводити оцінку (аудит) рівня захищеності державних інформаційних ресурсів, особливу увагу приділяючи тим, що підключені до мережі Інтернет. Це дозволить своєчасно виявити слабкі місця в системах захисту та вжити необхідних заходів для їх усунення.

З урахуванням глобальних викликів в сфері інформаційної безпеки, важливо, щоб національна система оцінювання захищеності державних інформаційних ресурсів відповідала міжнародним стандартам. Тому необхідно розробити нові нормативно-правові акти, які б дозволили інтегрувати кращі міжнародні практики та забезпечили ефективне оцінювання.

З метою попередження та мінімізації ризиків, пов'язаних з порушенням цілісності, доступності та конфіденційності державних інформаційних ресурсів, здійснюється комплекс заходів. До них належать розробка та впровадження ефективних систем виявлення інцидентів інформаційної безпеки, регулярне проведення аудиту систем захисту, навчання персоналу правилам інформаційної безпеки, а також розроблення планів реагування на інциденти. Крім того, проводиться постійна робота з аналізу загроз та вразливостей, що дозволяє своєчасно вживати необхідних заходів для усунення виявлених проблем.

Створення та розвиток українського CSIRT (Computer Security Incident Response Teams - структури швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів) є одним з ключових елементів державної політики у сфері кібербезпеки. Такий підрозділ зможе оперативно реагувати на кіберінциденти, що загрожують державним інформаційним ресурсам, проводити розслідування причин їх виникнення та розробляти заходи щодо запобігання подібних ситуацій у майбутньому. Це, в свою чергу, сприятиме підвищенню загального рівня захищеності національного інформаційного

простору та зміцненню кібербезпеки держави.

У сучасному світі, де інформація стала стратегічним ресурсом, захист інформації є невід'ємною складовою національної безпеки. Загрози інформаційній безпеці є різноманітними та постійно еволюціонують. Це можуть бути як зовнішні атаки з боку державних і недержавних акторів, так і внутрішні загрози, пов'язані з людським фактором, технічними збоями або природними катаклізмами. Реалізація цих загроз може призвести до значних політичних, економічних, соціальних та навіть військових наслідків. Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

1. Застосування технічних засобів для збору інформації про оборонні системи, економічні індикатори, наукові дослідження, дипломатичні переговори, а також для виявлення загроз національній безпеці

Сучасні технології дозволяють збирати розвідувальну інформацію за допомогою широкого спектру засобів, включаючи супутники, літаки, безпілотні літальні апарати, наземні станції та підводні човни. Ці системи здатні вести безперервне спостереження за територією України, фіксуючи різноманітні дані, від військових об’єктів до інфраструктурних проектів. Крім того, розвиток технологій штучного інтелекту значно підвищує ефективність аналізу великих обсягів даних, отриманих в результаті розвідки.

2. Несанкціонований доступ до інформації, що обробляється в інформаційних системах, а також цілеспрямовані дії, спрямовані на її спотворення, знищення чи блокування

Розширення використання інформаційно-телекомунікаційних систем в Україні супроводжується значним зростанням обсягів оброблюваної інформації та кількістю користувачів. Водночас, переважна більшість цих систем базується на іноземних технологіях, які не завжди забезпечують необхідний рівень захисту інформації. Це створює умови для кібератак, несанкціонованого доступу до даних, а також маніпуляцій з інформацією з метою дестабілізації суспільства та підриву національної безпеки.

3. Несанкціоноване отримання інформації з обмеженим доступом технічними каналами внаслідок електромагнітних випромінювань, які супроводжують роботу електронних пристроїв, або через акустичні та оптичні засоби підслуховування та спостереження.

Використання технічних засобів в інформаційній діяльності, хоча й полегшує роботу з інформацією, водночас створює додаткові ризики для її безпеки. Фізичні процеси, що супроводжують роботу комп'ютерної техніки та інших пристроїв, можуть призводити до витоку інформації через різноманітні технічні канали. Крім того, активне використання імпортних технічних засобів, які не завжди відповідають вимогам інформаційної безпеки, посилює цю проблему. Наявність іноземних представництв та можливість проведення розвідувальних заходів в безпосередній близькості від об'єктів інформаційної діяльності також створюють додаткові загрози.

Високий рівень вразливості інформації, особливо конфіденційної, вимагає від держави переходу до системного та комплексного підходу до забезпечення інформаційної безпеки. Необхідно створити єдину державну систему захисту інформації, починаючи з регіонального рівня та забезпечити її необхідними ресурсами й залучити висококваліфікованих фахівців. Лише за таких умов можна ефективно протидіяти сучасним інформаційним загрозам та захистити національні інтереси.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ОРГАНАХ ВЛАДИ РЕГІОНАЛЬНОГО РІВНЯ

3.1 Інформаційна безпека регіонального рівня

Зростаюча залежність регіональних органів влади від інформаційних технологій та систем управління, що базуються на обробці великих обсягів даних, значно підвищує значення інформаційної безпеки. Конфіденційність, цілісність та доступність інформації є критично важливими для ефективного функціонування органів влади та надання якісних послуг населенню. З іншого боку, зростає кількість загроз інформаційній безпеці, пов'язаних як з внутрішніми, так і з зовнішніми факторами. Це можуть бути як випадкові помилки персоналу, так і цілеспрямовані кібератаки, спрямовані на отримання несанкціонованого доступу до інформації, її модифікацію або знищення. Особливо вразливими є системи, що містять персональні дані громадян, комерційну таємницю, а також інформацію, що стосується національної безпеки.

Сумська область є однією з тих які щодня потерпають від атак не тільки з використанням фізичних засобів ураження, а й в інформаційному просторі.

Так наприклад за даними Відділу протидії кіберзлочина в Сумській області за перше півріччя 2024 року зафіксовано більше семисот випадків кібершахрайства, основним з яких є розсилка фішингових повідомлень.

За данними Державної служби спеціального зв’язку та захисту інформації України загальна кількість виявлених інцидентів збільшилась з 1463 за друге півріччя 2023 року до 1739 за перше півріччя 2024 року (рис. 3.1) (Державна служба спеціального зв’язку та захисту інформації, 2024). В свою чергу кількість атак на сектор безпеки і оборони зросла більш ніж вдвічі з 111 до 276 за аналогічні періоди (рис. 3.2). Також значно зросла кількість випадкиві

розповсюдження (рис 3.3) та зараження пристроїв шкідливим програмним забезпеченням (рис 3.4).

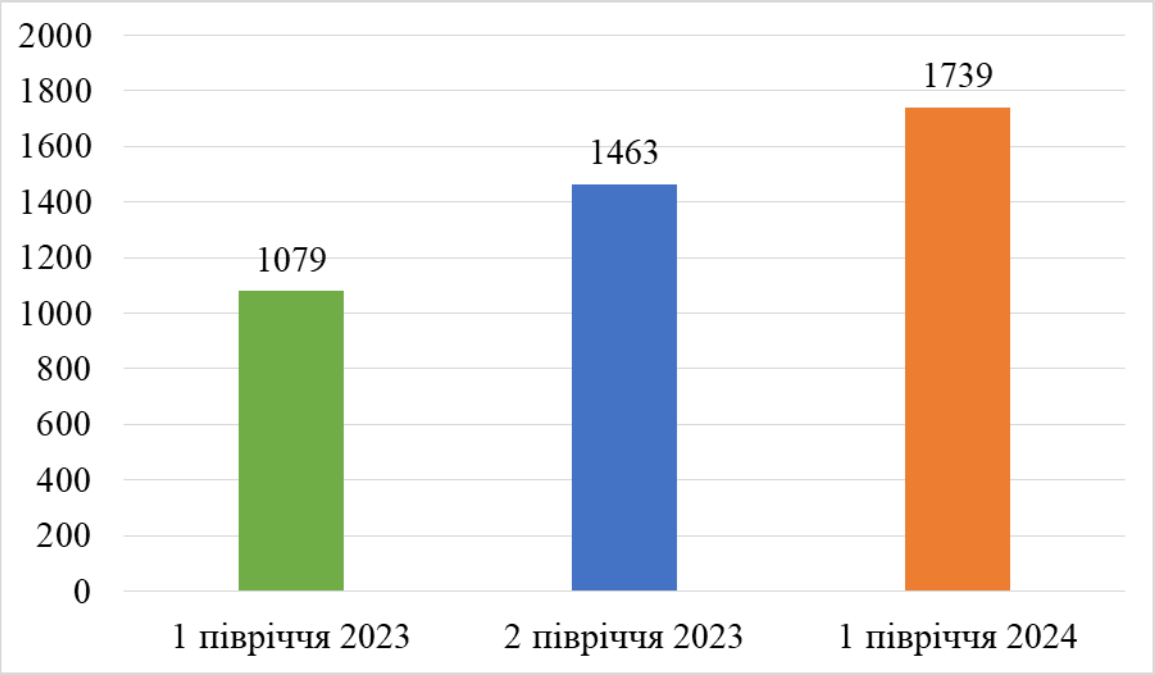

Рисунок 3.1 – Кількісні показники інцидентів за 2023 – 2024 роки

Джерело: узагальнено автором за даними Державної служби спеціального зв'язку та захисту інформації України

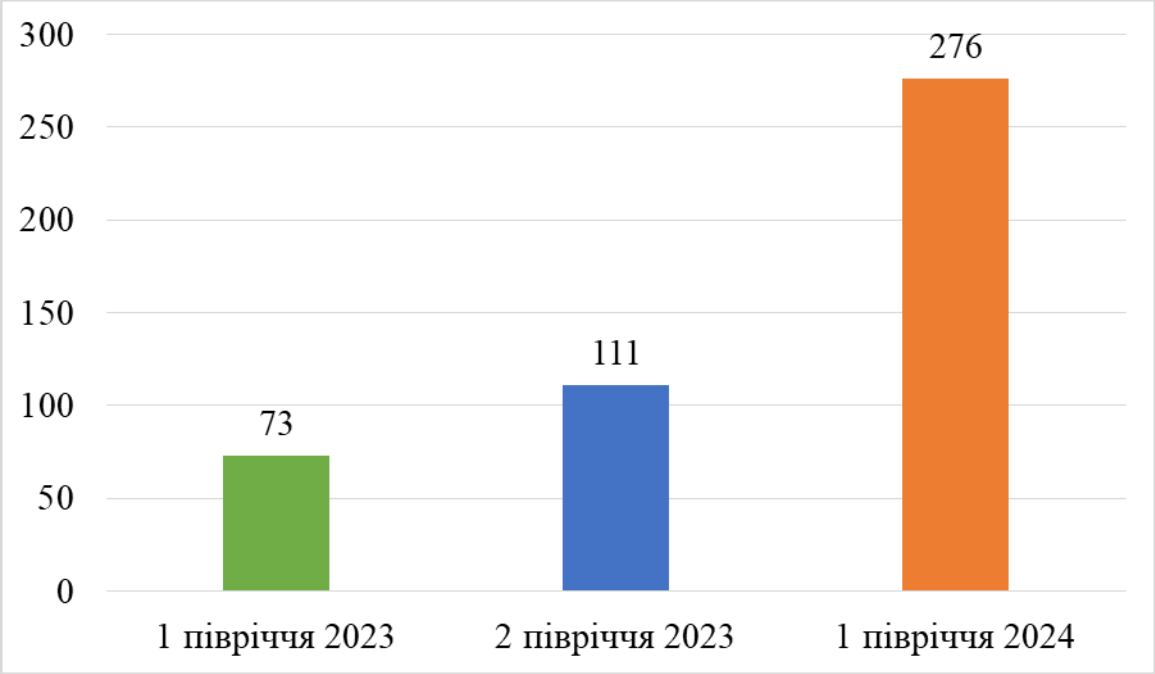

Рисунок 3.2 – Кількісні показники інцидентів в секторі безпеки та оборони за 2023 – 2024 роки

Джерело: узагальнено автором за даними Державної служби спеціального зв’язку та захисту інформації України

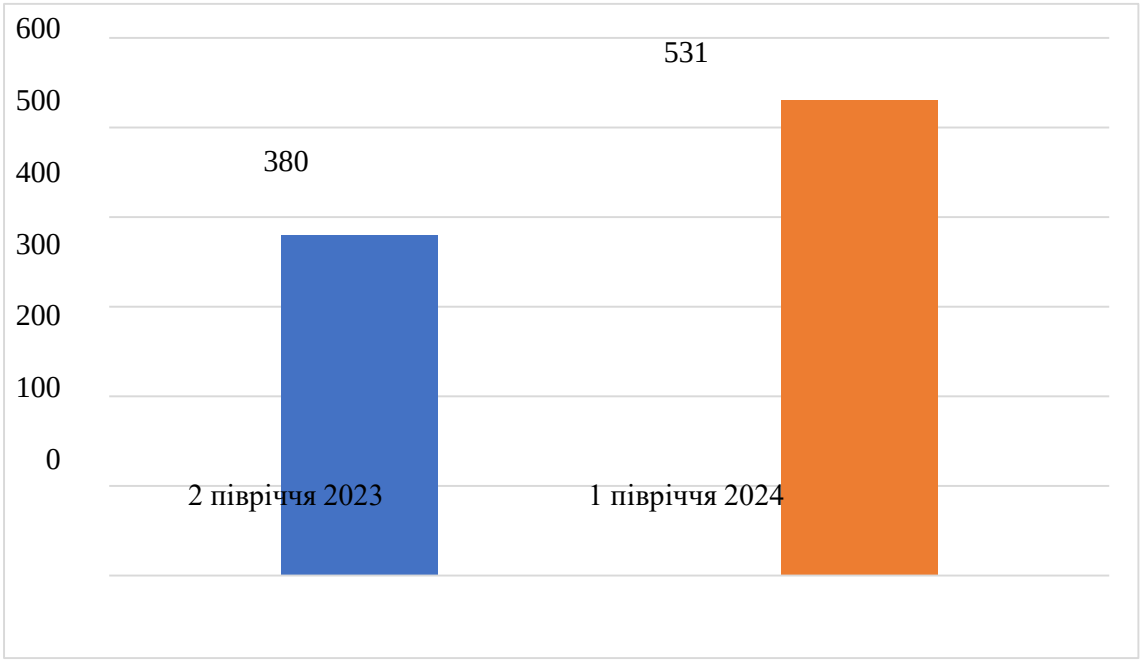

Рисунок 3.3 – Кількість інцидентів з розповсюдження шкідливого програмного забезпечення за 2023 – 2024 роки

Джерело: узагальнено автором за даними Державної служби спеціального зв’язку та захисту інформації України

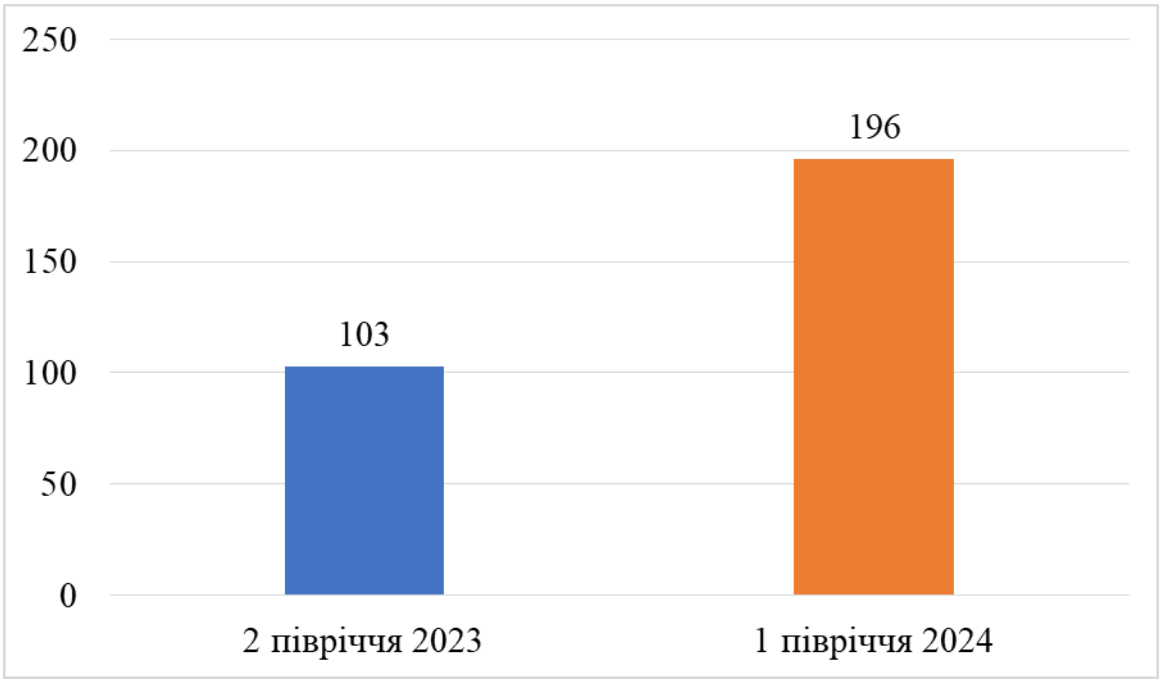

Рисунок 3.4 – Кількість інцидентів із зараження шкідливим програмним забезпечення за 2023 – 2024 роки

Джерело: узагальнено автором за даними Державної служби спеціального зв’язку та захисту інформації України

Одним з найпростіших кроків є впровадження політик інформаційної або кібербезпеки, як комплексного документу чи окремих політик, що регулюватимуть окремі елементи.

На цей час, за даними з відкритих джерел, жодного подібного нормативного документу на території області не існує, як в органах влади так і в комунальних установах.

Забезпечення інформаційної безпеки є критично важливим для успішного функціонування будь-якої організації, незалежно від її розміру та сфери діяльності. Крім стратегічних цілей, інформаційна безпека безпосередньо впливає на такі аспекти діяльності, як переговори, укладання контрактів, дослідження та розробки. Наявність у системі інформаційних потоків даних, що становлять державну таємницю, комерційну таємницю, персональні дані та іншу конфіденційну інформацію, значно підвищує ризики кібератак, шантажу, промислового шпигунства та інших видів злочинної діяльності. У випадку успішної атаки наслідки можуть бути катастрофічними: фінансові втрати, репутаційні ризики, втрата переваг, порушення законодавства та кримінальна відповідальність.

Так само як і на державному рівні, управління інформаційною безпекою на рівні регіонів має бути націлене на нейтралізацію різних видів загроз:

- Зовнішні загрози інформаційній безпеці, такі як кібератаки, шпигунство, недобросовісна конкуренція та збої в роботі глобальних інформаційних систем, створюють значні ризики для бізнесу, держави та суспільства в цілому. Дії злочинних угруповань та конкурентів можуть призвести до серйозних наслідків, включаючи втрату конфіденційної інформації, фінансові збитки та порушення репутації.
- внутрішніх, таких як помилки і халатність персоналу, а також навмисні дії, що призводять до порушень, збоїв і проблем в роботі власних інформаційних систем та ін.

Управління інформаційною безпекою в державному органі є складним і багатогранним процесом, який вимагає комплексного підходу. Кожен орган має свої унікальні особливості, пов'язані з характером його діяльності, обсягом та типом оброблюваної інформації, а також рівнем технологічної оснащеності. Тому система управління інформаційною безпекою повинна будуватися з урахуванням конкретних потреб кожного органу та постійно адаптуватися до змін зовнішнього середовища.

Забезпечення інформаційної безпеки в державних органах включає захист не тільки загальнодержавних видів таємниці, але й комерційної таємниці підприємств, перелік якої визначається підприємством самостійно згідно з законодавством. Це вимагає від державних органів врахування інтересів підприємств та встановлення тісної взаємодії з ними у сфері інформаційної безпеки.

3.2 Рекомендації щодо удосконалення системи управління інформаційною безпекою

З метою протидії сучасним кіберзагрозам та захисту конфіденційної інформації комерційні підприємства впроваджують систему менеджменту (управління) інформаційною безпекою. Такі системи дозволяють комплексно оцінювати ризики, розробляти ефективні заходи захисту та забезпечувати безперервну роботу інформаційних систем. В багатьох органах державного сектору, а особливо, на регіональному рівні варто застосовувати схожі підходи у зв’язку зі схожістю основних інформаційних процесів.

Пропонуємо впровадити системи менеджменту ІБ за декількома основними напрямами:

1) Розробити та реалізувати комплексні стратегії інформаційної безпеки, які передбачають створення багаторівневої системи захисту, що включає в себе розробку та впровадження детальних внутрішніх політик, процедур і стандартів.

2) Створити окремі та незалежні уповноважені підрозділи з інформаційної безпеки, а не просто покладання обов’язків на певну особу, як додаткове навантаження.

3) Сформувати сценарії та процедури на випадок непередбачених обставин.

4) Провести комплексні оцінку та аудит ефективності заходів безпеки.

Для ефективного функціонування систем інформаційної безпеки передбачити комплексну взаємодію різних елементів:

1) Політики та правила, розроблені уповноваженим підрозділом з інформаційної безпеки, встановлюють чіткі вимоги до поведінки персоналу при роботі з інформаційними ресурсами, визначають рівні доступу та відповідальність за збереження конфіденційності даних.

2) Відповідальність підрозділу ІБ за розробку та підтримку технічних заходів захисту, таких як системи виявлення вторгнень, фаєрволи та системи шифрування.

3) У разі виникнення інцидентів, має спрацьовувати система реагування, яка передбачає чітко визначені ролі та відповідальність, процедури ескалації та координації дій.

4) Регулярні аудити з метою оцінки ефективність заходів, дозволяють виявити потенційні вразливості та забезпечити відповідність системи захисту інформації встановленим стандартам.

5) За результатами аудиту розробляюти плани заходів для усунення виявлених недоліків та підвищення загального рівня безпеки.

Оскільки організаційна структура, процеси та зовнішнє середовище перебувають у постійному русі, завдання в кожному напрямку діяльності також мають бути динамічними. Регулярний аналіз змін та їх вплив на кожен напрямок дозволяє своєчасно виявляти нові виклики та можливості, а також коригувати завдання таким чином, щоб максимально ефективно досягати поставлених цілей. Такий підхід забезпечує не тільки адаптацію до змін, але й постійне вдосконалення всіх аспектів діяльності.

3.3. Принципи впровадження політики інформаційної безпеки

Політика інформаційної безпеки являє собою не просто набір правил, а скоріше детально розроблена стратегія, яка охоплює всі аспекти захисту інформації в організації. Вона слугує своєрідним компасом, що направляє всі дії, пов'язані із забезпеченням безпеки даних.

Для побудови дієвої політики безпеки пропонуємо виділити три основні рівні: верхній, середній і нижній.

Верхній рівень політики інформаційної безпеки має визначати загальну філософію та цілі інформаційної безпеки, відповідальність керівництва, принципи управління ризиками та вимоги до конфіденційності, цілісності та доступності інформації та має бути основою для розробки політик безпеки нижчих рівнів.

Політики інформаційної безпеки середнього рівня повинні конкретизувати загальні принципи, встановлюючи детальні правила та процедури для різних категорій співробітників, інформаційних систем та процесів за ступенем їх важливості. Необхідно встановити вимоги до інформаційних технологій, методів та підходів, що використовуються для обробки даних і створення нових інформаційних систем. Також на цьому рівні регламентують вимоги до співробітників, як ключових учасників процесів обробки інформації та відповідальність за її захист, а також встановити рівні допуску та доступу до ресурсів інформаційної системи.

Політики безпеки найнижчого рівня мають деталізувати особливості технічної реалізації захисту інформації. Визначають конкретні правила, процедури та технічні вимоги для окремих компонентів інформаційних систем, таких як сервери, мережі, бази даних, робочі станції тощо. Ці політики описують, як саме повинні бути налаштовані і захищені ці компоненти, щоб забезпечити загальну безпеку системи. Крім того, на цьому рівні визначають процедури резервного копіювання, відновлення даних, управління доступом до

окремих ресурсів та інші деталі, необхідні для ефективного функціонування системи захисту інформації.

Розробка ефективної політики безпеки вимагає ретельного підготовчого етапу, який повинен включати кілька важливих кроків.

1) Проведення оцінки ризиків притаманних установі. Це передбачає аналіз ставлення власників та керівництва до потенційних загроз, оскільки їхня готовність інвестувати в заходи безпеки безпосередньо впливає на рівень захисту інформації.

2) Детальний аналіз інформаційних активів установи. Необхідно визначити їх цінність та вразливість до різних типів загроз.

3) Проведення оцінки ризиків, пов'язаних з кожним ідентифікованим активом. Цей процес передбачає визначення потенційних загроз, ймовірності їх реалізації та можливих наслідків.

Результати оцінки та аналізу ризиків будуть основою для розробки конкретних заходів безпеки.

Аналіз інформаційної безпеки є постійним процесом, який необхідно проводити на постійній основі для оцінки ефективності вжитих заходів та адаптації стратегії до змін у внутрішньому та зовнішньому середовищі. Результати аналізу дозволяють виявити нові ризики, оцінити вразливість інформаційних систем та розробити заходи для їх усунення. При цьому важливо враховувати як об'єктивні дані, так і суб'єктивні оцінки керівництва, оскільки саме вони визначають стратегічні пріоритети організації.

Для забезпечення безпеки роботи з чутливими даними необхідна сувора регламентація всіх процесів. Політика інформаційної безпеки в даному випадку передбачає детальний опис технічних вимог (використання сертифікованого обладнання та програмного забезпечення), організаційних процедур (проходження процедур допуску, розподіл обов'язків) та фізичних заходів безпеки (обладнання спеціальних приміщень). Такий комплексний підхід дозволяє створити надійний бар'єр від несанкціонованого доступу до конфіденційної інформації та забезпечити її цілісність та доступність.

Розробляючи політики інформаційної безпеки на всіх рівнях, необхідно чітко дотримуватися принципу підпорядкованості. Політики нижчих рівнів повинні повністю відповідати вимогам політик вищих рівнів, а також чинного законодавства та нормативних актів. Текст та формулювання в політиках повинні бути чіткими, однозначними та не допускати двоякого тлумачення. Також тексти політик мають бути доступними для розуміння всім співробітникам, до яких вони звернені. Тільки за таких умов політика інформаційної безпеки може бути ефективним інструментом захисту інформаційних ресурсів організації.

Політика інформаційної безпеки є фундаментальним документом, який визначає правила поведінки всіх учасників інформаційних процесів в організації. Ефективна політика інформаційної безпеки є запорукою захисту інформаційних активів організації. Вона не тільки визначає технічні засоби захисту, але й формує культуру безпеки серед співробітників. Політика повинна чітко розподіляти відповідальність між усіма учасниками інформаційних процесів, забезпечуючи прозорість і зрозумілість правил. Політика не лише регламентує технічні аспекти захисту інформації, але й визначає процедури взаємодії між різними підрозділами та рівнями доступу до інформаційних ресурсів. Крім того, політика безпеки має забезпечувати захист не тільки інформації, а й прав користувачів, гарантуючи конфіденційність їхніх даних. Крім того, політика має бути адаптивною, тобто регулярно оновлюватися з урахуванням нових загроз та технологічних змін.

ВИСНОВКИ

В результаті аналізу законодавчих і інших нормативних вимог при захисті даних виявлено, що ні в Україні, ні в Сполучених Штатах Америки, ні в країнах ЄС не виявлено однозначних вимог щодо кіберзахисту даних. Вимоги щодо безпеки даних в ЄС та США значно ширші порівняно з українськми вимогами. В проєкті Закону України від 25 жовтня 2022 р. «Про захист персональних даних», який базується на положеннях GDPR врегульовано значну частину розбіжностей між національним та європейським законодавством. Прийняття цього проекту значно покращить нормативно-правове регулювання захисту персональних даних в Україні. До недоліків цього проекту можна віднести відсутність системи регулювання обробки персональних даних неповнолітніх. Також в проекті відсутні вимоги до інформаційно-комунікаційних систем, в яких обробляються та циркулюють критичні дані.

Постійні несанкціоновані втручання в роботу автоматизованих та інформаційних систем органів державної влади, об’єктів критичної інфраструктури, підприємств, установ та організацій різних форм власності та підпорядкування, призводять до значних збоїв у роботі та наносять велткі втрати громадянам, бізнесу та державі вцілому.

Ризик виникнення інцидентів кібербезпеки значним чином можна зменшити сформувавши відповідні рекомендації для суб’єктів даних та осіб, що обробляють цю інформацію в тому числі в органах державної влади. Також необхідним є розробка політик, щодо функціонування компонентів інформаційних систем обробки даних, а також відповідальних за їх експлуатацію, враховуючи особливості діяльності органів державної влади.

З проведеного аналізу та дослідження видно, що система інформаційної безпеки в державних органах є законодавчо та нормативно врегульованою, однак може бути покращена шляхом прийняття додаткових нормативних документів як центральними органами так і регіональними.

Інформаційна безпека в центральних органах влади забезпечується та підтримується Службою безпеки України та Адміністрацією державної служби спеціального зв’язку та захисту інформації.

На регіональному рівні одним з рекомендованих та необхідних методів удосконалення СУІБ є впровадження, прийняття та введення в дію політик інформаційної безпеки, як для окремих установ виходячи зі специфіки діяльності так і регіональних, базуючись на потребах регіону в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію, Закон України № 2657-XII (1992) (Україна). https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99. (1999) (Україна). https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки, Закон України № 537-V (2007) (Україна). https://zakon.rada.gov.ua/laws/show/537-16#Text.

4. Yu Zhang, Haoyun Dong. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing*, volume 12, Article number: 64 (2023). https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-023-00437-3#citeas.

5. Brown, R., Truby, J. & Ibrahim, I.A. Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. European Studies, 2022, Sciendo, vol. 9 no. 1, pp. 61-90. https://doi.org/10.2478/eustu-2022-0003

6. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (2016) (Європейський союз). https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

7. Троценко С. І., Снігуров А. В. Розробка підходу до забезпечення інформаційної безпеки осіб з урахуванням інформації соціальних мереж. *Системи обробки інформації.* 2014. Вип. 2. С. 137–142.

8. Romansky, Radi. (2023). Internet of Things and User Privacy Protection. *37th International Conference on Information Technologies, InfoTech 2023* – Proceedings. http://infotech-bg.com/proceedings.

9. Кальченко В., Ободяк В. Порівняльна характеристика нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах. *Наукові праці міжрегіональної академії управління персоналом*. *Інформаційні технології та суспільство*. 2023. Випуск 5 (11). С. 14 – 20.

10. Кальченко, В. В., Ободяк В. К., Пугач І.О. Нормативні вимоги України в сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах у порівнянні з вимогами США та ЄС. *Вісник Херсонського національного технічного університету*. 2024. № 2. С. 162 – 169.

11. Puhach, I., Liubchak, V. (2024). Management of information security of critical infrastructure objects. Інформаційні технології і автоматизація – 2024. Видавництво ОНТУ. С. 156 – 157.

12. Пугач, І. О., Таранюк, К. В. (2024). Нормативне регулювання інформаційної безпеки в органах державної влади. Інформаційні технології і автоматизація – 2024. Видавництво ОНТУ. С. 217 – 219.

13. Про доступ до публічної інформації, Закон України № 2939-VI (2011) (Україна). https://zakon.rada.gov.ua/laws/show/2939-17#Text

14. Конституція України, № 254к/96-ВР (1996) (Україна). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

15. Про захист персональних даних, Закон України № 2297-VI (2010) (Україна). https://zakon.rada.gov.ua/laws/show/2297-17#Text

16. Про захист інформації в інформаційно-комунікаційних системах, Закон України №80/94-ВР (2010) (Україна). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

17. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанова Кабінету Міністрів України № 518 (2019) (Україна). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

18. Про затвердження документів у сфері захисту персональних даних. Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 (2014) (Україна). https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.

19. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова Кабінету Міністрів України № 373 (2006) (Україна). https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

20. Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Постанова Кабінету Міністрів України від № 1106 (2017) (Україна). https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text

21. Про захист персональних даних. Проект Закону України № 5628 (2021) (Україна). https://itd.rada.gov.ua/billInfo/Bills/Card/26873.

22. Про захист персональних даних. Проект Закону України № 8153 (2022) (Україна). https://itd.rada.gov.ua/billInfo/Bills/Card/40707.

23. Federal Act concerning the Protection of Personal Data (DSG) (2019) (Germany). https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

24. Act on the implementation of the general data protection regulation (2018) (Croatia). https://azop.hr/national-legislation/.

25. Act about the processing of personal data. Act of the Czech Republic №110 (2019) (Czech Republic) https://www.zakonyprolidi.cz/translation/cs/2019-110?langid=1033&srcid=1029.

26. Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven). Dansk lov nr 502 (2018) (Danmark). https://www.retsinformation.dk/eli/lta/2018/502.

27. La loi Informatique et Libertés. Loi de la France non 78-17 (1978) (France). https://www.cnil.fr/fr/la-loi-informatique-et-libertes.

28. Federal Data Protection Act (BDSG). Act of Germany (2019) (Germany). https://www.gesetze-im-internet.de/englisch_bdsg/index.html.

29. Data protection act 2018. Act of Ireland № 7 (2018) (Ireland). https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.

30. Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Act of Italy №101 (2018) (Italy) https://www.garanteprivacy.it/codice.

31. Uitvoeringswet Algemene verordening gegevensbescherming. Nederlandse wet (2021) (Nederland) https://wetten.overheid.nl/BWBR0040940/2021-07-01.

32. The Act on the Protection of Personal Data. Act of Poland (2018) (Poland) https://uodo.gov.pl/en/660/1464.

33. Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. ley Española no 294 (2018) (España). https://www.boe.es/eli/es/lo/2018/12/05/3.

34. Lag med kompletterande bestämmelser till EU:s dataskyddsförordning. Sveriges Lag 2018:218 (2018) (Sverige). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/.

35. Data Protection Act. Act of Finland 1050/2018 (2018) (Finland). https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.

36. Law on legal protection of personal data. Republic of Lithuania law № I-1374 (1996) (Republic of Lithuania). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae.

37. Mantelero, A., Vaciago, G., Esposito, M. S., Monte N. The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, 2020, 28, 297–328 https://academic.oup.com/ijlit/article/28/4/297/6120059?login=false.

38. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending

Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing. Directive 2007/64/EC. Directive of EU 2015/2366 (2015) (European Union). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

39. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Regulation of EU 910/2014 (2014) (European Union). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

40. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Directive 2007/64/EC. Directive of EU 2022/2555 (2022) (European Union). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1704742816799.

41. The Privacy Act of 1974. Act of USA (1974) (USA). https://www.archives.gov/about/laws/privacy-act-1974.html.

42. California Consumer Privacy Act of 2018. Act of California (2018) (USA). https://cppa.ca.gov/regulations/pdf/cppa_act.pdf.

43. The Civil Code of California. Act of California (1872) (USA). https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV&tocTitle=+Civil+Code+-+CIV.

44. NIST Privacy Framework: a tool for improving privacy through enterprise risk management, version 1.0. https://doi.org/10.6028/NIST.CSWP.01162020.

45. Овсяний, К. (2023, 7 грудня). Під наглядом Кремля: Спецслужби РФ роками отримували відео з тисяч камер спостереження по всій Україні? Радіо Свобода. https://www.radiosvoboda.org/a/skhemy-kamery-sposterezhennya-trassir-kreml/32718775.html

46. Міністерство цифрової трансформації України. (2024, квітень 21) Індекс цифрової трансформації регіонів України 2023.

https://hromada.gov.ua/research/indeks-cifrovoyi-transformaciyi-regioniv-ukrayini-2023

47. Axelos. Information Technology Infrastructure Library (ITIL). https://www.axelos.com/certifications/itil-service-management/

48. Information Systems Audit and Control Association. Control Objectives for Information Technologies (COBIT). https://www.isaca.org/resources/cobit

49. International Organization for Standardization/ International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022). https://www.iso.org/ru/standard/27001

50. European Union Agency for Network and Information Security. Information security management system framework. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework

51. International Organization for Standardization/ International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022). https://www.iso.org/ru/standard/27002

52. Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 45 (2023) (Україна). https://zakon.rada.gov.ua/laws/show/z0320-07#Text

53. Російські кібероперації. Аналітика за 1 півріччя 2024 року, Державна служба спеціального та захисту інформації, https://cip.gov.ua/ua/news/cyber-operations-rf-h1-2024-report

ДОДАТОК А

Таблиця А.1– Числові значення індексів цифрової трансформації

Назва області	Значення індексу
Загалом для України	0,632
Дніпропетровська	0,908
Львівська	0,891
Полтавська	0,833
Волинська	0,831
Тернопільська	0,827
Харківська	0,787
Одеська	0,785
Вінницька	0,777
Закарпатська	0,732
Рівненська	0,727
Івано-Франківська	0,685
Київська	0,684
Черкаська	0,672
Хмельницька	0,620
Житомирська	0,560
Чернігівська	0,553
Чернівецька	0,546
Кіровоградська	0,531
Миколаївська	0,441
Луганська	0,404
Донецька	0,359
Херсонська	0,316
Запорізька	0,289
Сумська	0,178
Автономна Республіка Крим	0,000

Таблиця А.2 – Значення субіндексів цифрової трансформації регіонів

Область	Субіндекс							
	Інституційна спроможність	Розвиток інтернету	Розвиток ЦНАП	Впровадження режиму без паперів	Цифрова освіта	Візитівка області	Проникнення базових е-послуг	Галузева ЦТ
Вінницька	0,900	0,784	0,712	0,868	0,920	0,600	0,551	0,848
Волинська	0,880	0,870	0,808	0,865	0,624	0,900	0,947	0,747
Дніпропетровська	1,000	0,902	0,908	0,923	0,968	1,000	0,901	0,826
Донецька	0,320	0,118	0,369	0,605	0,546	0,600	0,569	0,272
Житомирська	0,380	0,769	0,515	0,743	0,552	0,100	0,566	0,511
Закарпатська	0,800	0,602	0,683	0,813	0,820	1,000	0,847	0,688
Запорізька	0,598	0,185	0,432	0,141	0,658	0,050	0,428	0,065
Івано-Франківська	0,900	0,769	0,643	0,599	0,240	0,600	0,610	0,690
Київська	0,685	0,689	0,744	0,718	0,542	1,000	0,728	0,534
Кіровоградська	0,320	0,619	0,589	0,622	0,524	0,500	0,528	0,454
Львівська	0,880	0,914	0,905	0,951	0,840	0,600	0,885	0,918
Миколаївська	0,167	0,609	0,510	0,487	0,656	0,900	0,534	0,105
Одеська	1,000	0,849	0,706	0,819	0,620	1,000	0,904	0,601
Полтавська	0,800	0,917	0,709	0,902	0,936	1,000	0,738	0,836
Рівненська	0,960	0,609	0,653	0,853	0,472	1,000	0,733	0,732
Сумська	0,300	0,173	0,066	0,182	0,398	0,000	0,416	0,104
Тернопільська	1,000	0,916	0,747	0,856	0,732	1,000	0,672	0,773
Харківська	0,728	0,926	0,696	0,809	0,968	0,500	0,809	0,773
Херсонська	0,286	0,179	0,383	0,612	0,834	0,500	0,286	0,092
Хмельницька	0,800	0,756	0,504	0,667	0,458	0,100	0,664	0,637
Черкаська	0,656	0,595	0,711	0,731	0,686	0,500	0,687	0,719
Чернівецька	0,500	0,374	0,733	0,740	0,546	0,500	0,589	0,447
Чернігівська	0,612	0,404	0,630	0,536	0,546	0,600	0,720	0,509