Міністерство освіти і науки України
Університет митної справи та фінансів

Факультет управління
Кафедра публічного управління та митного адміністрування

Дипломна робота магістра

на тему: Механізми публічного управління забезпечення кібербезпеки в сучасних умовах

Виконав: студент групи ПУ22 – 1зм
Спеціальність 281 "Публічне управління та адміністрування"
Бондаренко В. О.

Керівник: к.держ.упр., доцент, Ковальов В. Г.

Рецензент: _____
(місце роботи)
_____
(посада)
_____
(науковий ступінь, вчене звання, прізвище та ініціали)

Дніпро – 2024

АНОТАЦІЯ

Бондаренко В.О. **Механізми публічного управління забезпечення кібербезпеки в сучасних умовах**

Дипломна робота на здобуття освітнього ступеня магістр за спеціальністю 281 «Публічне управління та адміністрування». Університет митної справи та фінансів, Дніпро, 2024.

Метою магістерської роботи є дослідження теоретичних основ та надання практичних рекомендацій з вдосконалення механізмів публічного управління у сфері кібербезпеки в сучасних умовах.

У роботі досліджено здійснено аналіз теоретичних підходів до визначення поняття кібербезпека та його місця в системі публічного управління. Досліджено нормативно – правове регулювання публічного управління кібербезпекою. Розглянуто зарубіжний досвід щодо публічного управління забезпечення кібербезпеки. Визначено практичні особливості застосування механізмів публічного управління обміном інформацією щодо кібератак, кіберінцедентів та інцидентів безпеки інформації. Проаналізувано роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 – 2023 років. Охарактеризовано результати співробітництва органів публічної влади України з Європейським союзом у сфері кібербезпеки. За результатами дослідження надано рекомендації щодо удосконалення проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Сформовано пропозиції щодо внесення змін до законодавчих актів із підвищення рівня кібербезпеки.

Ключові слова: публічне управління, механізми, забезпечення кібербепеки, інформаційно-комунікаційні технології, сучасні умови.

SUMMARY

Bondarenko V.O. Mechanisms of public management to ensure cyber security in modern conditions

Graduate work for obtaining an educational degree by a Master's degree in specialty 281 "Public Administration". University of Customs and Finance, Dnipro, 2024.

The purpose of the master's thesis is to study the theoretical foundations and provide practical recommendations for improving the mechanisms of public management in the field of cyber security in modern conditions.

In this work the analysis of theoretical approaches to the definition of the concept of cyber security and its place in the system of public administration is carried out. Normative and legal regulation of public management of cyber security has been studied. Foreign experience regarding public management of cyber security is considered. The practical features of the application of mechanisms for public management of information exchange regarding cyberattacks, cyber incidents and information security incidents have been determined. The work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks during the years 2022 - 2023 was analyzed. The results of cooperation between public authorities of Ukraine and the European Union in the field of cyber security are characterized. Based on the results of the study, recommendations were made for improving the review of cyber protection of state information resources and critical information infrastructure.

Keywords: public administration, mechanisms, ensuring cyber security, information and communication technologies, modern conditions.

Список публікацій здобувача:

1. Бондаренко В.О. Механізми публічного управління забезпечення кібербезпеки в сучасних умовах // Економіко – правові та управлінсько – технологічні виміри сьогодення: молодіжний погляд: матер. міжнар. наук.-практ. конф. (м.Дніпро, листопад 2023). Дніпро: УМСФ, 2023.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІКТ	Інформаційно-комунікаційні технології
НАТО	Організація Північноатлантичного договору
ЄС	Європейський Союз
ІБ	Інформаційна безпека
ІКСТ	Інформаційно-комунікаційні системи і технології
ОЗКБ	Основні засади забезпечення кібербезпеки України
Держспецзв'язку	Державна служба спеціального зв'язку та захисту інформації України
КСЗІ	Комплексна система захисту інформації
ENISA	European Network and Information Security Agency (Європейська агенція з безпеки мереж та інформації; ЄС)
ШПЗ	Шпигунське програмне забезпечення
ІТС	Інформаційно-телекомунікаційна система
РНБО	Рада національної безпеки і оборони
ОКІ	Об’єкт критичної інфраструктури
ОКІІ	Об’єкт критичної інформаційної інфраструктури
ДПП	Державно – приватне партнерство

ВСТУП

Актуальність дослідження. Сьогодення вимагає від кожної країни відповідності своїх спроможностей у захисті конституційних прав та свобод своїх громадян, особливо в тих сферах суспільних відносин, де застосовність продукції інформаційно-комунікаційних технологій має визначальний вплив на життєво важливі послуги, ведення бізнесу, безпеку всіх видів комунікацій, життєдіяльності громадян, суспільства та держави. Крім того, проникнення таких технологій у повсякденне життя вимагає нових знань в новому середовищі – кіберпросторі, від якого слід очікувати не тільки великої кількості сервісів та благ, а й розвитку існуючих та створення нових загроз. Ці загрози пов’язані із застосуванням механізмів несанкціонованого втручання в роботу систем та порушення безпеки інформації, яку вони обробляють, постійний розвиток індустрії розроблення та широке використання різного роду шкідливого та уразливостей широковживаного програмного забезпечення, застосування спеціальних операцій у кіберпросторі на об’єкти критичної інформаційної інфраструктури тощо.

Пильна увага громадськості до питань впровадження цифрових технологій в широкий спектр суспільних відносин, щоденно зростаюча небезпека від їх використання робить актуальним завдання системного дослідження національної системи кібербезпеки, її вад, обґрунтування напрямків та завдань щодо її модернізації.

Вітчизняними науковцями здійснювались дослідження різних аспектів публічного управління кібербезпеки України: О. Бакалінською, О. Бакалинським, Л. Веселовою, Ю. Геращенко, О. Ю. Горуном, М.М. Сливкою, Т. Станіславським, Л.М. Дешко та К.Д. Бонарєвою, В.В. Бухарєвим, В.А. Лахно, Б.В. Бистровою, А.Ю. Шинкаренко, О.В. Ставицьким, С.Г. Петровим. Деякі аспекти зазначеної проблематики потребують додаткового вивчення та доопрацювання, зокрема підвищення ефективності взаємодії суб’єктів державної системи забезпечення кібербезпеки та адаптації вітчизняної системи в реагування на кіберінциденти міжнародним стандартам.

Мета і завдання дослідження. Метою магістерської роботи є дослідження теоретичних основ та надання практичних рекомендацій з вдосконалення механізмів публічного управління у сфері кібербезпеки в сучасних умовах.

Для досягнення поставленої мети було визначено такі завдання:

– здійснити аналіз теоретичних підходів до визначення поняття кібербезпека та його місця в системі публічного управління;

– дослідити нормативно – правове регулювання публічного управління кібербезпекою;

– розглянути зарубіжний досвід щодо публічного управління забезпечення кібербезпеки;

– визначити практичні особливості застосування механізмів публічного управління обміном інформацією щодо кібератак, кіберінцедентів та інцидентів безпеки інформації;

– проаналізувати роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 – 2023 років;

– охарактеризувати результати співробітництва органів публічної влади України з Європейським союзом у сфері кібербезпеки;

– надати рекомендації щодо удосконалення проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

– сформувати пропозиції щодо внесення змін до законодавчих актів із підвищення рівня кібербезпеки та інформатизації;

– визначити вплив державно – приватного партнерства на перспективи розвитку механізмів захищеності інформації та інформаційно-телекомунікаційних систем.

Об’єкт дослідження – публічна політика у сфері кібербезпеки України.

Предмет – механізми публічного управління забезпечення кібербезпеки в сучасних умовах.

Методи дослідження. Для досягнення мети використано загальнонаукові методи: порівняння та систематизація – при зборі інформації для аналізу норм національних законодавств у сфері кібербезпеки та аналізі статистичних даних про події інформаційної безпеки України потягом 2022 – 2023 рр., узагальнення – для оцінки діючого механізму державного регулювання кіберзахистом та дослідження можливостей впровадження міжнародного досвіду, системний підхід – для формування пропозицій щодо удосконалення механізмів публічного управління кіберзахистом в Україні, логічний метод – для теоретичного узагальнення та формулювання висновків, графічний метод – для наочного представлення тенденцій розвитку досліджуваних явищ.

Методологічною базою дослідження є наукові праці вітчизняних та зарубіжних дослідників, офіційні публікації міжнародних організацій. Інформаційну базу дослідження сформували нормативні документи органів публічної влади, статистичні дані системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, матеріали, опубліковані в періодичних виданнях та мережі Інтернет.

Апробація результатів дипломної роботи. Результати кваліфікаційної роботи магістра пройшли апробацію на Міжнародній науково-практичній конференції «Економіко – правові та управлінсько – технологічні виміри сьогодення: молодіжний погляд» від 03 листопада 2023 року, Університет митної справи та фінансів, м. Дніпро.

Структура та обсяг дипломної роботи. Логіка проведеного дослідження зумовила структуру роботи: вступ, три розділи (дев’ять підрозділів), висновки, список використаних джерел. Загальний обсяг роботи становить 85 сторінок, Список використаних джерел налічує 53 найменувань, у тому числі 10 іноземною мовою. У роботі вміщено 21 рисунків та 7 таблиць. Положення тексту доповнює матеріал, викладений в 5 додатках.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1. Теоретичні підходи до визначення поняття кібербезпека та його місця в системі публічного управління

В епоху глобальних викликів інформація та інформаційні технології є основним стратегічним національним ресурсом, що визначає економічну та оборонну могутність держави. Вони мають вирішальне значення для кожного аспекту існування суспільства, включаючи банківську справу та фінанси, науку, освіту, транспорт і зв'язок, енергетику та оборону, виробництво та управління та багато інших сфер. При цьому недостатня захищеність державної таємниці призводить до витоку політичної, економічної та військової інформації. На сьогоднішній день глобальні та регіональні інформаційні суперечності, вразлтвість баз данніх, загострення інформаційної війни, захист національних інформаційних ресурсів та гарантія інформаційної безпеки виступають першочерговими стратегічними задачами будь – якої країни. Захист інформаційної незалежності, особливо в мережі Інтернет, забезпечення ефективного функціонування системи обміну данних є актуальним завданням державної політики кібербезпеки. Доступ до стабільного та безпечного цифрового середовища має гарантувати держава, яка є охоронцем прав і свобод громадян.

Останнім часом суспільство дедалі частіше стикається з різноманітними видами атак: при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, порушення цілісності та конфіденційності даних, інформаційно – психологічний тиск на населенняшпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для

економіки та безпеки держави підприємств, систем життєзабезпечення й об’єктів підвищеної небезпеки.

Відповідно до зазначеної проблематик більшої уваги вітчизняних урядовців та наукових привертає поняття «кібербезпека», якк з’явилося ще на початку 80-х років. У праці американського вченого - інформатика Б. Томаса розглядаються проблеми безпеки, які пов’язані з загрозами телекомунікацій та інформатики і вразливості ком’ютерних систем. На сьогоднішній день існують чимало різних трактувань сутності кібербезпеки (таблиця 1.1).

Таблиця 1.1

Характеристика поняття «кібербезпека» у працях вітчизняних дослідників

Автори	Трактування поняття «кібербезпека»
Бакалінська О., Бакалинський О. [1, С. 102]	захист віртуального середовища, що виникло внаслідок появи Інтернету, а також діяльності людей та організацій на технологічних пристроях та мережах, які до нього підключені
Веселова Л. [2, С. 25]	захист критично важливих інфраструктурних послуг сприяє основним потребам безпеки, зокрема: – безпека інформації стосується захисту конфіденційності, цілісності та доступності інформації загалом, щоб задовольнити потреби відповідного користувача інформації; – безпека мережі стосується проектування, впровадження та функціонування мереж для досягнення цілей безпеки інформації в мережах в межах організацій, між організаціями та між організаціями та користувачами; – безпека Інтернету стосується захисту послуг, пов'язаних з Інтернетом, та пов'язаних із ними ІКТ-систем та мереж як розширення безпеки мережі в організаціях та вдома; – захист критичної інформаційної інфраструктури займається захистом систем, за допомогою яких об’єктами критичної інфраструктури надаються життєво необхідні послуги: енергетичні, телекомунікаційні системи та водоканали
Геращенко Ю. [3, С. 141]	збір політик та дій, які використовуються для захисту підключених мереж (у тому числі комп’ютери, пристрої, апаратне забезпечення, збережена інформація та інформація, що передається) від несанкціонованого доступу, модифікації, крадіжок, зриву, переривання чи інших загроз
Горун О. Ю. [4, С. 95]	сукупність інструментів, політик, концепцій безпеки, запевнень в безпеці, настанови, підходи до управління ризиками, дії, навчання, кращі практики, забезпечення та технології, які можна використовувати для захисту кіберсередовища, активів організації та користувача

Об'єктом кібербезпеки є інформаційні ресурси, технології їх формування і використання, а також інфраструктура комп'ютерних мережа, яка використовується для створення інформації, її збору, обробки, накопичення, зберігання, поширення і надання споживачам. Суб'єктом – окремі особистості, група людей, організації, органи державної влади або окремі посадові особи, які порушують своїми діями конфіденційність, цілісність або доступність інформації в цифровому просторі, тобто приносять шкоди об'єкту інформаційної безпеки [5, С. 180]. Схематично модель взаємодії підсистеми кіберзахисту у складі системи забезпечення кібербезпеки та іншими її складовими наведена в Додатку Б.

Як зазначає у своїй роботі М.М. Сливка, вітчизняний вектор державно політики в галузі інформаційно – комунікаційних технологій (ІКТ – далі) значно спирається на міжнародне співробітництво у сфері забезпечення кібернетичної безпеки, взаємодію з питань кібербезпеки за участі органів державної влади України і відповідних органів Північноатлантичного альянсу (НАТО – далі) шляхом співпраці на двосторонній основі, упровадження інформаційно – комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування на кіберінциденти, в цілому інтеграції Національної системи кібербезпеки до відповідних систем Європейського Союзу (ЄС – далі) та НАТО, затвердження акредитації з боку Національного центру кіберзахисту та протидії кіберзагрозам [6, С. 490].

Т. Станіславський, розвиваючи цю ідею, доходить висновку, що кібербезпека є пріоритетом у діяльності не тільки різних держав, а й їх регіональних об’єднань і навіть всієї світової спільноти, а міжнародне співробітництво має мати системний і послідовний характер, супроводжуватися грунтовними дослідженнями [7, С. 60].

Л.М. Дешко та К.Д. Бонарєва підкреслюють важливість міжнародного співробітництва в галузі державного управління кібербезпекою для Україні, однак констатують, що існуючий нормативно – правовий (імплентація Будапештської конвенції про кіберзлочинність, Угода про реалізацію

Трастового фонду Україна – НАТО тощо) та організаційно-правовий механізми співпраці (Україна – ЄС та Україна – НАТО та інші) не повною мірою відповідають викликам, з якими стикається система державного управління сьогодні [8, С. 139].

Закономірно невирішені проблеми приваблють увагу численної кількості вітчизняних науковців, які присвячують свої праці питанням розвитку та впровадження механізмів регулювання функціонування системи кібербезпеки нашої держави і реалізації національної кібербезпекової політики надається не на стільки значна увага. В.В. Бухарєвим розглянуто адміністративно – правові форми забезпечення кібербезпеки в Україні як зовнішнє вираження діяльності уповноважених органів державної влади, яке виявляється у вивченні ними комплексу дій, що спрямовані на створення таких умов, за яких буде забезпечено безпеку комп'ютерних систем. Зазначається, що адміністративний договір як адміністративно – правова форма забезпечення кібербезпеки являє собою добровільну угоду між декількома суб'єктами адміністративного права, які наділені владними повноваженнями, з метою координації їхньої спільної діяльності та яка в підсумку приводить до виникнення, зміни або припинення взаємних прав та обов'язків сторін відповідного договору. За допомогою адміністративного договору вбачається можливим скоординувати роботу різних державних структур, однак лише у випадках, коли в цьому існує об'єктивна необхідність [9, С. 76].

В роботі В.А. Лахно досліджено особливості державного регулювання інформаційно – комунікаційного середовища транспорту та зазначено орієнтацію на взаємодію з іншими секторами економіки для скорочення затримок при транспортуванні вантажів, обробці морських і річкових суден, контейнерів, залізничних вагонів і вантажів на прикордонних переходах на основі використання систем електронних накладних, системи «клієнтбанк», e-business, взаємодії із клієнтурою й партнерами тощо. Критичність виходу з ладу систем такого рівня складності вимагає нових підходів системи державного управління до питань забезпечення інформаційної безпеки з

акцентом на доступність та стійкість систем, а також цілісності інформації, яка зберігається та опрацьовується в інформаційних системах та автоматизованих системах керування галузі. Стаття містить результати досліджень, які спрямовані на подальший розвиток методів розпізнавання органами державної влади, залученими в управління системою кібербезпеки держави, загроз інформаційно-комунікаційним системам і технологіям (ІКСТ – далі) та удосконалення інформаційної безпеки (ІБ – далі) в умовах формування єдиного інформаційно – комунікаційного середовища, впровадження нових та модернізації існуючих інформаційним системам і збільшення кількості дестабілізуючих впливів на доступність, схоронність і цілісність інформації. Запропоновано метод розпізнавання загроз на основі дискретних процедур з використанням апарату логічних функцій та нечітких множин, що дозволяє підвищити ефективність розпізнавання, створювати ефективні програмні рішення для систем захисту інформаційних ресурсів ІКСТ [10, С. 46].

Б.В. Бистрова проводить порівняльний аналіз державної політики у сфері вищої освіти та підготовки фахівців з кібербезпеки, порівнюючи реалії вітчизняних реалій з передовим досвідом навчання за схожими освітньопрофесійними програмами у вищих навчальних закладах Сполучених Штатах Америки. Визначенр, що професійна підготовка фахівців з кібербезпеки є однією зі складових національної безпеки, без якої є неможливими захищене передавання інформації в умовах інформаційних війн, замахів на цілісність і суверенітет держави. Практична підготовка в американських реалізується на засадах інтегративного поєднання навчання в університеті та здобуття практичних навичок на майбутньому робочому місці, з отриманням заробітної плати. В той час, як українські виші не мають такої можливості щодо отримання досвіду роботи – здобувачі самостійно організовують місце проходження практики [11].

А.Ю. Шинкаренком та О.В. Ставицьким досліджено основні чинники, що впливають на ймовірність економічної структури стати жертвою кібератаки. Розглянуто і проаналізовано основні шляхи, інструменти і

механізми реалізації кібератак. У цій роботі проаналізовано причини і наслідки останніх наймасштабніших атак у кіберпросторі, які мали місце відбутися на території України і які були спрямовані, у тому числі, на стратегічно важливі для розвитку національної економіки структури, проаналізовано основні механізми та інструменти захисту інформації. Визначено доцільність витрат спрямованих на захист інформації, стратегічно важливої для розвитку будь – якої економічної структури [12].

С.Г. Петровим визначено основні чинники, які зумовлюють, а також впливають на ймовірність кібератак; проаналізувати можливі наслідки, які можуть бути спричинені внаслідок успішних кібератак; з’ясувати ймовірні витрати на механізми безпеки інформації. Також авторами зазначається, що зломи інформаційно – комунікаційних систем стосуються великих організацій, то останні, як правило, потрапляють під приціл громадських засобів масової інформації. Однак вони становлять лише невеликий відсоток від загальної кількості атак, які відбуваються щороку. У той час як малі та середні підприємства часто орендують віддалені сервери, великі організації зазвичай зберігають дані на власних носіях. Для більшості представників малого та середнього бізнесу зломи несуть важкі наслідки [13, С. 21].

Варто зауважити, що широке впровадження комп'ютерних технологій в усі сфери життя сучасного суспільства підвищило його вразливість для протиправних дій та викликали стрімке зростання комп'ютерних злочинів. Вихід в глобальну мережу Інтернет тягне за собою загрози інформаційній безпеці національних комп'ютерних систем. Перш за все, це несанкціонований доступ до інформаційних ресурсів, а також їх можливе руйнування. Використання імпортних інформаційних технологій в автоматизованих системах управління різними без прийняття відповідних заходів щодо забезпечення інформаційної безпеки створює реальні загрози національній безпеці України [14, С. 64]. Відповідно за зазначеної проблематики, в Україні на державному рівні реалізується низка заходів із забезпечення кібербезпеки вітчизняних інформаційних систем та баз даних (рис.1.1).

Рис.1.1. Шари захисту кібурбезпеки [14]

Таким чином, на основі аналізу трактувань різними авторами сутності поняття «кібербезпека» можна стверджувати, що захист важливих цифрових систем та баз даних від несанкціонованого доступу є важливою передумовою для розвитку сучасного суспільства, а своєчасне виявлення, запобігання та нейтралізація реальних або потенційних загроз національній безпеки України в кіберпросторі сприяє вдосконаленню політики забезпечення безпеки в цифровому просторі країни. Окільки урядові, військові, фінансові та медичні організації збирають, обробляють та зберігають велику кількість стратегічно важливих даних, питання їх захисту є приоритетом системи публічного управління в галузі кібербезпеки, для захисту якої розроблена низка законодавчих актів та імплементовані міжнародні стандарти.

1.2. Нормативно – правове регулювання механізмів публічного управління кібербезпекою

Відповідність системи кібербезпеки сучасним викликам та загрозам, її збалансованість на основі впровадження принципів мінімально необхідного регулювання (пропорційності та адекватності заходів кібербезпеки), максимально можливого застосування норм національного та міжнародного права, невтручання у приватне життя і захисту персональних даних, рівнозначності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури та інших є головним завданням публічної політики в сфері кібербезпеки та кіберзахисту.

Закон «Про основні засади забезпечення кібербезпеки України» [15] (ОЗКБ – далі) за своїм змістом та сутністю є ключовою складовою розвитку сфери кібербезпеки та кіберзахисту. Він визначає категорійно-понятійний апарат, об'єкти, суб'єкти та принципи кібербезпеки, об'єкти кіберзахисту, структуру Національної системи кібербезпеки та завдання її основних складових, механізми державно-приватного та державно-суспільного партнерства тощо. В ст. 3 визначена загальна ієрархія законодавчих актів, які формалізують публічну політику в цій сфері, а саме: «Правову основу забезпечення кібербезпеки України становлять Конституція України [16], Законів України «Про національну безпеку України» [17] та «Про Доктрину інформаційної безпеки України» [18], Конвенції про кіберзлочинність [19], а також засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України» [15].

Особливістю сфери кібербезпеки є висока динаміка змін, які відбуваються в ній і які значною мірою обумовлені динамікою розвитку ІКТ, збільшенням кількості та рівня складності кіберзагроз, способів, методів і інструментів протидії їм. Ця особливість обмежує терміни дії стратегічних

документів з кібербезпеки та кіберзахисту, які з часом швидко втрачають свою актуальність і тому не повинні розроблятись на термін більш ніж 3-5 років

Оскільки кібербезпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави, яка з одного боку, передбачає забезпечення якісного всебічного вільного доступу до різних джерел інформації в мережі Інтернет, а з іншого – це контроль за непоширенням шкідливого програмного забезпечення. Вкрай актуальною з точки зору повноти державного управління кібербезпекою є прийняття законопроекту «Про безпеку критичної інфраструктури та її захист» [22], що займає важливе місце в системі нормативно – правових актів, які присвячені забезпеченню безпеки цифрового простору України (рис.1.2).

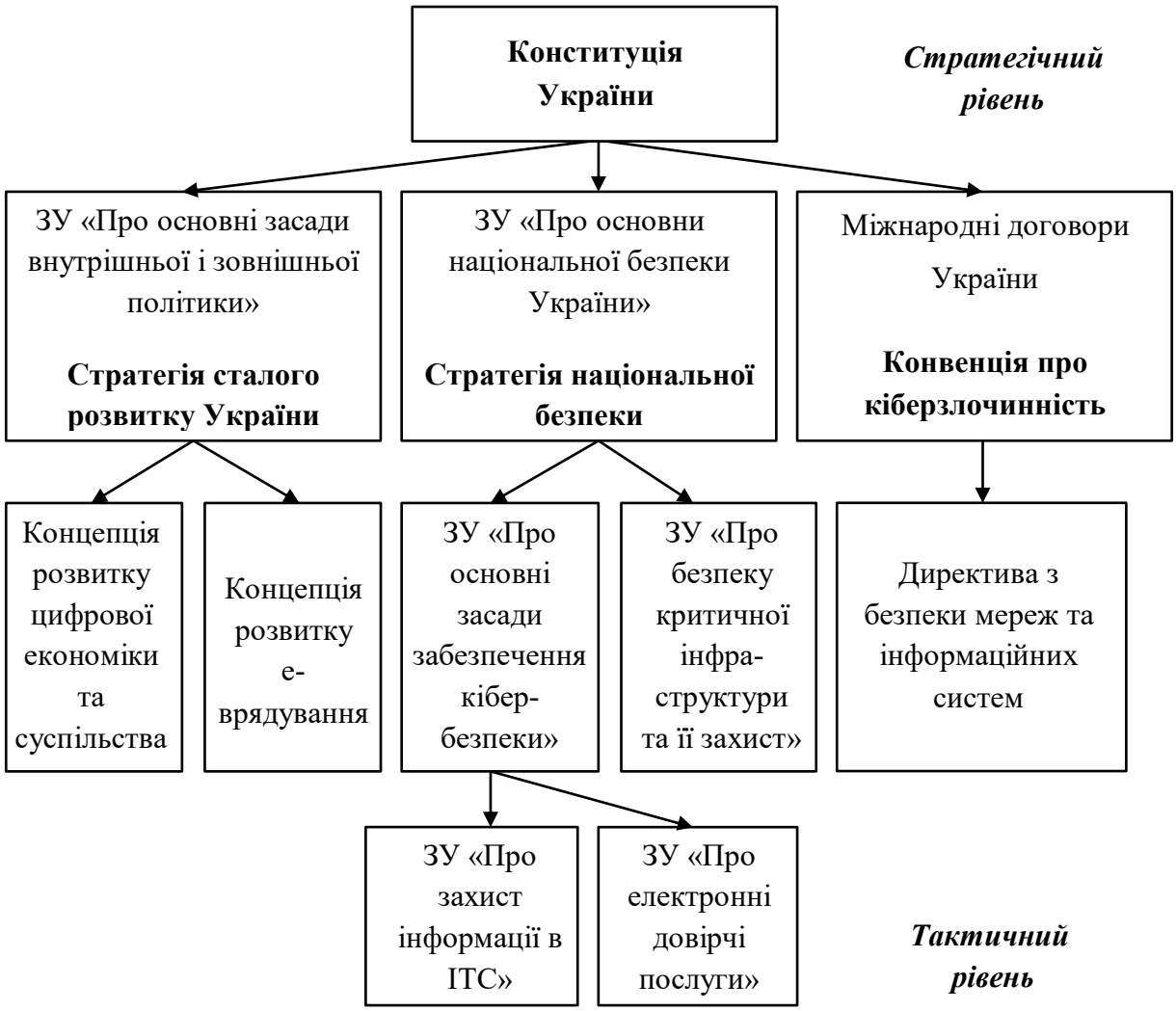


Рис. 1.2. Схема нормативно-правового забезпечення кібербезпеки України [15 – 22]

В Законі ОЗКБ надається визначення «Стратегії кібербезпеки України», вказується її місце в системі довгострокових документів з питань національної безпеки і оборони, розкривається узагальнена структура змісту, а також визначені головні суб'єкти, що відповідають за кібербезпеку та кіберзахист [15]. В проекті закону «Про безпеку критичної інфраструктури та її захист», основним призначенням якого є визначення повноважень, завдань та відповідальності суб'єктів державної системи захисту критичної інфраструктури, передбачено врегулювання комплексу питань, більшість з яких відносяться до стратегічного планування та управління в цій сфері [21]:

– створення державної системи захисту критичної інфраструктури;

– визначення повноважень складових сектору безпеки і оборони, які повинні передбачати забезпечення оборони, провадження правоохоронної, розвідувальної, контррозвідувальної діяльності, контртерористичний захист та кіберзахист критичної інфраструктури, захист економічного та науково-технічного потенціалу держави, обмін інформацією з питань оцінки загроз та реагування на загрози і кризові ситуації, а також ліквідації їх наслідків у взаємодії з іншими суб'єктами державної системи захисту критичної інфраструктури;

– встановлення стандартизованого процесу виявлення та зменшення ризиків для життєво важливої інфраструктури, зокрема щодо нещасних випадків і технологічних збоїв, небезпечних подій і незаконної діяльності;

– визначення стандартів і процесу визначення об'єктів інфраструктури як критичної інфраструктури, а також кроків, пов'язаних із їх сертифікацією та класифікацією;

– визначення засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури;

– здійснення міжнародного співробітництва у сфері захисту критичної інформаційної інфраструктури.

В Законі ОЗКБ [15] визначені як суб'єкти забезпечення кібербезпеки взагалі, так і основні суб'єкти національної системи кібербезпеки зокрема з їх

конкретними завданнями, а також система органів що здійснює їх координацію (табл.1.2).

Таблиця 1.2

Ключові елементи Стратегії кібербезпеки України [15]

Об’єкти механізму забезпечення кібербезпеки держави			
Діяльність правоохоронних органів	Діяльність суб’єктів формування державної політики	Комунікаційні системи	Відомчі комунікаційні системи
Публічні, приватні та суспільні інтереси	Конституційні права і свободи людини і громадянина	Комунікаційні системи державного органу	Комунікаційні системи міжнародних органів
Професійна діяльність держслужбовів	Інтереси членів сімей держслужбовців	Об’єкти критичної інформаційної інфраструктури державного органу	
Суб’єкти забезпечення кібербезпеки держави			
Міністерство цифрової трансформації України	Міністерство внутрішніх справ України	Служби внутрішньої безпеки	Міністерство оборони України та Генеральний штаб Збройних Сил
Кіберполіція	Служба безпеки України	Держслужба спеціального зв’язку та захисту інформації України	
Принципи механізму забезпечення кібербезпеки			
Законність	Ієрархічність	Конфіденційність	Доступність
Приватність	Захист даних	Комплексність	Систематичність
Завдання механізму забезпечення кібербезпеки			
Протидія кіберзагрозам	Забезпечення обмеженого доступу до даних	Забезпечення безпеки даних	Забезпечення безпеки особистих даних
Забезпечення безпеки особистих даних співробітників	Формування системи реагування на кіберзагрози	Формування забезпечення реалізації механізму	Здійснення оцінки ефективності кібербезпеки

Зміст положень закону повною мірою відповідає своїй назві і визначає: правові та організаційні основи забезпечення захисту у кіберпросторі; основні цілі, напрями та принципи державної політики; повноваження суб’єктів та

основні засади координації їх діяльності. У зв’язку з цим, очікувати від нього запровадження регулювання суспільних відносин у сфері кібербезпеки не виправдано [15].

В Законі досить ретельно виписані елементи забезпечення кібербезпеки, їх функції та завдання, але досить поверхньо виписана організація їх взаємодії або координація. Практика застосування його норм вказує на необхідність посилення саме цієї частини закону, більш чіткого виписування норм, які б забезпечили утворення саме екосистеми кібербезпеки України. При цьому сфера дії закону не поширювалась на системи, де циркулює секретна інформація, і вимагає пошуку нових організаційних форм та технічних механізмів, використання яких досвідченими у сфері кібербезпеки фахівцями забезпечило б безпеку мереж та інформації, які в них обробляються.

Основні завдання координації основних суб’єктів кібербезпеки України, до преліку яких, по суті, увійшов весь силовий блок, покладені на робочий орган Ради національної безпеки та оборони України у сфері кібербезпеки – національний координаційний центр кібербезпеки, розвитку спроможностей якого належна увага приділена не була. У зв’язку з цим, основною формою роботи цього центру стало прийняття на своїх засіданнях доручень для інших державних органів. Основна увага з цих органів приділялася Державній службі спеціального зв'язку та захисту інформації України – спеціально уповноваженому центральному органу виконавчої влади у сфері спеціального зв’язку та захисту інформації. Тобто, спостерігалась стала тенденція щодо застосування механізмів законодавства суміжної сфери – захисту інформації – для вирішення завдань кібербезпеки. Враховуючи, що кібербезпека є специфічною частино системи гарантування безпеки інформації, існуючі вади механізмів сфери захисту інформації знайшли своє повторення при вирішенні завдань кібербезпеки, основною з яких є наявність завдання, але відсутність норми щодо регулярного перегляду запроваджених механізмів захисту інформації новим загрозам. Ця проблема в подальшому призвела до руйнації сутності комплексної системи захисту інформації– системи, яку треба постіно

підтримувати в адекватному загрозам стані – відповідності безпеки інформації, яка з використанням механізмів КСЗІ досягається [37]. Завдання системи державного управління кібербезпекою систематизовано в таблиці 1.2.

Таблиця 1.2

Завдання системи державного управління кібербезпекою України [15]

Ключові завдання системи державного управління кібербезпекою України		
1. Оцінка кібербезпеки та кіберзахисту державного органу	2. Оцінка потенційних кіберзагроз на майбутні періоди	3. Формування нормативів забезпечення кібербезпеки державного органу
– аналіз критичних точок; – визначення шляхів здійснення хакерських атак; – ідентифікація найбільш вразливих місць; – аналіз та оцінка хакерських атак минулих періодів	– тестування інформаційної системи; – аналіз розвитку кіберпростору та кіберзлочинності в Україні та світі; – оцінка хакерських атак в Україні та світі; – діяльність хакерських груп, та оцінку інших загроз Національній безпеці	– розробка та впровадження Положення про кібербезпеку та кіберзахист державного органу; – впровадження Протоколу протидії хакерським атакам; – розробка та впровадження Положення про оцінку наслідків хакерським атакам
4. Організація системи кіберзахисту	5. Організація безпеки особистих даних	6. Організація кібербпеки робочого місця
– встановленні відповідальних осіб за підтримку кіберзахисту; – організація постійного моніторингу за кіберзагрозами	– забезпечення безпеки особистих даних співробітників	– організація періодичного моніторингу за кіберзагрозами на робочому місці; – визначення порядку дій співробітника
7. Організація кібеззахисту процесів діяльності державного органу	8. Організація системи спеціального зв’язку на випадок несанкціонованого проникнення в інформаційну систему	9. Впровадження протоколу знищення даних на випадок фізичного проникнення
– організація захисту каналів зв’язку між співробітниками	– налагодження системи спеціального зв’язку системи управління	– порядок знищення матеріальних носіїв інформації

З метою якісного формування переліку об’єктів критичної інформаційної інфраструктури (комунікаційні і технологічні системи об’єктів критичної інфраструктури, технологічна інформація) та їх внесення до

Державного реєстру об’єктів критичної інформаційної інфраструктури, з урахуванням секторального підходу та міжнародного досвіду до системи державних органів, що мають надавати Державній службі спеціального зв'язку та захисту інформації України (Держспецзв’язку – далі) за встановленою формою галузеві переліки об’єктів критичної інформаційної інфраструктури включено [23]:

– Міністерство інфраструктури України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі транспорту;

– Міністерство економічного розвитку і торгівлі України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі хімічної промисловості або які включені до переліку підприємств, що мають стратегічне значення для економіки і національної безпеки держави (або безпеки населення та держави);

– Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в сферах життєзабезпечення населення, зокрема централізованого водопостачання, водовідведення, постачання електричної енергії і газу, є комунальними службами;

– Міністерство аграрної політики та продовольства України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги у сферах життєзабезпечення населення, зокрема у сферах виробництва продуктів харчування, сільського господарства, топографо-геодезичної та картографічної діяльності, ведення

– Міністерство охорони здоров'я України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги у сферах життєзабезпечення населення, зокрема у сфері охорони здоров’я;

– Міністерство внутрішніх справ України – щодо підприємств, установ і організацій незалежно від форми власності, які є об'єктами потенційно небезпечних технологій і виробництв, є аварійними та рятувальними службами;

– Міністерство юстиції України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги щодо технічного, технологічного забезпечення створення та супроводження програмного забезпечення ведення автоматизованих систем Єдиних та Державних реєстрів, здійснення заходів із супроводження програмного забезпечення системи реалізації майна, технологічного забезпечення, збереження та захисту даних, що містяться у ній, на організацію та проведення електронних торгів, торгів за фіксованою ціною та на виконання інших функцій, передбачених «Порядком реалізації арештованого майна»;

– Національний банк України – щодо підприємств, установ і організацій банківської системи незалежно від форми власності;

– Міністерство цифрової трансформації – щодо системи електронної взаємодії органів виконавчої влади, системи електронної взаємодії державних електронних інформаційних ресурсів, а також підприємств і організацій незалежно від форми власності, які забезпечують функціонування державних електронних інформаційних ресурсів;

– Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі електронних комунікацій.

При цьому необхідно підкреслити що формування та забезпечення функціонування Державного реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України здійснюються Національним банком України незалежно від органів виконавчої влади.

Два останніх державних органи є основними джерелами інформації про перелік об’єктів критичної інфраструктури сектору телекомунікації та зв’язку і включають [23]:

– операторів та провайдерів телекомунікацій, які мають важливе значення для функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, становити загрозу для життя і здоров’я людей, зокрема ті, які надають послуги доступу до мережі Інтернет власникам (розпорядникам) ІТС;

– державні електронні реєстри та їх технологічні складові, інформаційно-телекомунікаційні системи, кадастри, державні інформаційні системи незалежно від технології їх побудови, системи електронних торгів, системи державних тендерних закупівель;

– адміністраторів адресного простору мережі Інтернет у домені.UA;

– операторів цифрових послуг;

– операторів доступу до систем з використанням технологій «хмарних» обчислень;

– операторів послуг обміном Інтрнет-трафіком тощо.

Інформація про стан об’єктів інформаційної критичної інфраструктури збирається вищевказаними державними органами та використовується як при формуванні (корегуванні) Стратегії кібербезпеки України [22] та інших стратегічних документів, так і для оперативного реагування системою кібербезпеки на кіберінценденти та кібератаки. Організаційні питання координації з розробки, прийняття та виконання стратегічних рішень з питань кібербезпеки та кіберзахисту визначено в Законі ОЗКБ [15]:

– координація діяльності у сфер і кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України;

– Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони.

Узагальнену систему взаємодії органів державного управління кібербезпекою в Україні, покладені на неї завдання та оцінку результатів їх діяльності наведено в таблиці 1.3.

Таблиця 1.3

Порядок забезпечення кібербезпеки України [15; 23]

Порядок забезпечення кібербезпеки України		
1. Оцінка кібербезпеки, в цілому	2. Оцінка потенційних кіберзагроз на майбутні періоди	3. Формування Стратегії забезпечення кібербезпеки правоохоронної системи
Суб'єкти реалізації процесу		
1) Міністерство цифрової трансформації; 2) правоохоронних органів; 3) Кіберполіція; 4) Держслужба спеціального зв'язку та захисту інформації України; 5) Служби внутрішньої безпеки	1) Служби внутрішньої безпеки; 2) Кіберполіція; 3) Кабінет Міністрів України	1) Офіс Президента України; 2) Міністерство внутрішніх справ; 3) Міністерство цифрової трансформації; 4) Міжнародні інституції, що фінансуватимуть реалізацію стратегії
Результативний документ		
Звіт про реалізацію заходів забезпечення кібербезпеки, який надається суб'єктам реалізації державної політики в сферах правоохоронної системи, кібербезпеки національної безпеки.	Пояснювальні записки щодо: заходи щодо протидії кібератакам; виявленні критичні точки та можливий витік інформації; наслідки витоку інформації для публічних, суспільних та приватних інтересів; виявленні відхилень в реалізації стратегії	Звіт про заходи з реалізації стратегії, який містить інформацію про: заходи, що були реалізовані; відхилення та пояснення їх причин; ресурсне забезпечення та відхилення із причинами; коригування стратегічних заходів на наступні періоди

Однак законодачно неврегульованим залишається питання забезпечення взаємодії між Національним координаційним центром кібербезпеки, Державним центром кіберзахисту та протидії кіберзагрозам Держспецзв'язку, Урядовою командою реагування на комп'ютерні надзвичайні події України

CERT-UA та іншими командами реагування на комп’ютерні надзвичайні події, а також їх взаємодія з міжнародними центрами кіберзахисту. Виокремлюючи операційну та стратегічну діяльність вищевказаних суб’єктів кібербезпеки та кіберзахисту пропонується такий координаційний механізм: координацію операційної діяльності команд реагування, їх облік та опублікування на загальнодоступних ресурсах усіх контактних даних для зв’язку з ними, інформування уповноважених з питань обміну інформацією про кіберінциденти органів інших країн, здійснює Державна служба спеціального зв'язку та захисту інформації України [25].

Проаналізовані основні акти законодавства, що визначають розвиток національної системи кібербезпеки дали змогу сформувати ієрархічну інфраструктуру законодавства у сфері кібербезпеки з метою впорядкування та систематизації, в також викремити напрямки, в яких здійснюється законодавча діяльність,зокрема: формування та забезпечення функціонування Державного реєстру об’єктів критичної інформаційної інфраструктури; розробка нормативно – правових актів, які регламентують діяльність основних суб’єктів кібербезпеки України, їх конкретні завданн, а також формують систему органів що здійснює їх координацію; процедури збору інформації про стан об’єктів інформаційної критичної інфраструктури та оперативного реагування системою кібербезпеки на кіберінценденти та кібератаки. Забезпечення взаємодії між групами реагування на комп’ютерні надзвичайні ситуації, а також їх взаємодії з глобальними центрами кіберзахисту, залишається викликом. Пропонується наступний механізм взаємодії: координація оперативної діяльності груп реагування, облік та публікація на публічних ресурсах усієї контактної інформації для зв’язку з ними та інформування уповноважених осіб. Також, оскільки актуальною залишається проблема розробки та впровадження організаційно-правових механізмів управління розвитком кіберзахисту критичної інформаційної інфраструктури України, доцільним є врахуванням міжнародного досвіду в цій сфері, насамперед країн Європейського Союзу.

1.3. Зарубіжний досвід публічного управління забезпечення кібербезпеки

Сучасний світ, у тому числі й інформаційний, надзвичайно різноманітний у всіх своїх проявах. На даний час в різних країнах по-своєму трактують свободу слова і недоторканність приватного життя, свободу інформації, дії державної влади, громадськості, громадян і засобів масової інформації в цифровому просторі. При цьому у вітчизняному політичному і науковому співтоваристві бракує чіткого уявлення про наслідки такої політики і можливості використання зарубіжного досвіду в Україні. Як наслідок, врахування досвіду різних країн у формуванні та реалізації державної інформаційної політики може надати істотну допомогу політичному керівництву, громадськості та наукової спільноти в Україні.

Соціальний та економічний розвиток все більше залежать від швидкого та безперешкодного доступу інформації та її використання в управлінні, виробництві та сфері послуг та громадськості суб'єктів. Безперервний розвиток мережевих та інформаційних систем, включаючи аналіз даних, допомагає розвивати комунікації, торгівлю, транспорт або фінансові послуги. Будь-яке значне порушення функціонування інформаційного простору матиме вплив на економічну активність населення і його безпеку, ефективність державного сектора економіки, процеси виробництва та обслуговування, і в кінцевому рахунку – на національну безпеку. На сьогоднішній день існує ризик порушення цілісності та конфіденційності інформації, у тому числі навмисних нападів у вигляді зловмисного програмного забезпечення, злому інформаційно- телекомунікаційних систем або блокування надання послуг. Зловмисниками можуть бути як злочинні групи, що мають на меті фінансову вигоду або бути підтримані іноземними державами [25, С. 107].

Сучасна інформаційна політика в розвинених країнах – це сукупність напрямів і способів діяльності компетентних органів держави з контролю, регулювання та планування процесів у сфері одержання, зберігання,

оброблення, використання та поширення інформації. Держава регулює відповідний розподіл інформаційних ресурсів, загальні принципи інформаційної діяльності, встановлює пріоритети для забезпечення національних інтересів. Власну інформаційну політику ведуть більшість держав світу, але обсяги їхньої діяльності в цій сфері залежать від поставлених завдань і рівня зацікавленості конкретної країни в інтеграції до глобальної системи комунікації, від історичних чинників, політичного й економічного розвитку, фінансових і матеріальних ресурсів [26].

Забезпечення інформаційної безпеки є проблемою для всіх суб'єктів, які формують національну інформаційну безпеку, тобто суб'єктів господарювання, що надають послуги з використанням систем ІКТ, користувачів, державних органів, а також спеціалізованих установ, що займаються інформаційною безпекою на операційному рівні. Тому на даний час доволі важливим є міжнародне співробітництво між державами в рамках таких організацій, як ЄС та НАТО. Ця співпраця відіграє важливу роль у боротьбі зі зростаючою кількістю інцидентів, викликаних незаконною діяльністю в інформаційному просторі, що призводить до матеріальних і репутаційних збитків. Розвинені країни нині рухаються шляхом цілеспрямованого правового впорядкування відносин у національному інформаційному просторі, приймають необхідні законодавчі акти, перебудовують діяльність органів державної влади, які відповідають за формування та реалізацію інформаційної політики. Аналіз провідних концепцій дозволяє побачити здобутки і перспективи у цій сфері [26].

Щодо органів, які забезпечують інформаційну безпеку, то у ЄС у 2004 році було створено Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA – далі) надає практичні поради та рішення для державного та приватного секторів в країнах ЄС. Це включає: сприяння розробці національних стратегій; сприяння співробітництву між командами з реагування на надзвичайні ситуації та розбудови потенціалу. ENISA допомагає розробити політику та законодавство ЄС з питань мережевої та

інформаційної безпеки. Щоденна робота ENISA визначається щорічною робочою програмою Агентства, яка складається щороку після широких консультацій з керівництвом та виконавчою радою ENISA [27].

Європейський центр кіберзлочинності було створено у 2013 році для посилення реагування правоохоронних органів на кіберзлочинність в ЄС і таким чином сприяє захисту європейських громадян, підприємств та урядів від злочинів в мережі Інтернет. З моменту свого створення, Європейський центр кіберзлочинності вніс значний внесок у боротьбу з кіберзлочинністю. Щороку Європейський центр кіберзлочинності публікує Оцінку загрози організованої злочинності в Інтернеті, її головний стратегічний звіт про основні висновки та нові загрози та події в сфері кіберзлочинності [27].

10 грудня 2018 року Європейський Парламент та Європейська Комісія досягли політичної домовленості щодо Закону про кібербезпеку, який посилює повноваження ENISA для надання кращої підтримки держав-членів у боротьбі з загрозами у сфері кібербезпеки. Закон також встановлює рамки ЄС для сертифікації кібербезпеки, що підвищує безпеку онлайнових послуг та споживчих пристроїв. Закон про кібербезпеку включає виділення агентству більше ресурсів для надання йому змогу виконати свої завдання; посилення бази для ENISA в новій системі сертифікації кібербезпеки для надання допомоги державам-членам у ефективному реагуванні на кібер-атаки.

Цілями створення такої Агенції встановлено такі: впроваджувати та розвивати високий рівень експертиз; допомагати європейським інституціям, органам, офісам і агенціям розробляти політики безпеки мереж та інформації; допомагати впроваджувати необхідні політики для досягнення необхідних вимог, встановлених існуючими та в майбутньому розробленими актами; розвивати спроможності у підготовці до упередження, виявлення та реагування на проблеми, пов'язані з безпекою мереж та інформації, підтримувати закордонну кооперацію між учасниками державних органів та приватного сектору [27]. Практику державної політики інформаційної безпеки деяких держав Європейського Союзу наведено у табл. 1.4.

Таблиця 1.4

Практика державної політики кібербезпеки деяких держав Європейського Союзу [28 – 32]

Австрія	Національні стратегії побудовані на основі всеосяжного і інтегрованого підходу до забезпечення інформаційної безпеки	Стратегія спрямована на забезпечення безпеки інформаційного простору в країні	Керівна група з кібербезпеки Експертний центр з питань кіберзлочинності Австрійський центр кібербезпеки
Велика Британія	Національна стратегія кібербезпеки 2021 – 2026 включає набір планів, що ґрунтуються на роботі з приватним сектором	Стратегія спрямована на запобігання та зменшення впливу кібератак на Великобританію	Центр по боротьбі з експлуатацією та захисту дітей в Інтернеті Управління кібербезпеки та інформаційного забезпечення
Естонія	Національна стратегія кібербезпеки базується на комплексному підході до забезпечення інформаційної безпеки	Стратегія спрямована на полегшення використання інформаційних технологій та забезпечення їх безпеки	Управління інформаційних систем
Іспанія	Національна стратегія кібербезпеки має на меті створити адекватний потенціал для запобігання, захисту, виявлення, реагування та відновлення інформації	Стратегія спрямована на забезпечення безпеки інформаційного простору в країні та посилення її конкурентоспроможності	Національний центр розвідки Рада національної безпеки Спеціалізований комітет з кібербезпеки
Італія	Національна стратегія щодо безпеки кіберпростору є інтегрованими, структурованими та гнучкими	Стратегія спрямована на запобігання майбутнім загрозам в інформаційній сфері стабільність країни	Комітет з інформаційного суспільства Міністерство з інновацій та технологій Комітет з інформатизації держ установ
Німеччина	Національна стратегія кібербезпеки базується на комплексному підході до забезпечення інформаційної безпеки	Стратегія спрямована на підтримку та сприяння соціально-економічного розвитку Німеччини за рахунок інформаційних технологій	Офіцер захисту даних Національний центр кіберзахисту Національна рада кібербезпеки

В рамках своєї Стратегії кібербезпеки Австрія переслідує такі стратегічні цілі: наявність, надійність і конфіденційність обміну даними, а також цілісність самих даних; віртуальний простір повинен бути здатний протистояти ризикам, поглинати удари і регулювати до зміни середовища; розробка ключових систем ІКТ; на основі національного підходу компетентних федеральних міністерств Австрія забезпечить розвиток інфраструктури ІКТ; забезпечення високого рівня доступності, цілісності та конфіденційності необхідних інфраструктур ІКТ; Австрія відіграватиме активну роль у міжнародному співробітництві [28, С. 25].

Крім цього, в Австрії прийнято Національну стратегію безпеки ІКТ, яка передбачає такі стратегічні цілі та заходи:

1. Оптимізація числа зацікавлених сторін у сфері кібербезпеки в Австрії;
2. Налагодження зацікавлених сторін із інформаційною структурою;
3. Підвищення безпеки в інформаційному просторі;
4. Сприяння міжнародній співпраці [28, С. 26].

У Великобританії діє Закон про захист даних, який контролює, як особисті дані людини використовуються організаціями, підприємствами або урядом. Кожна особа, відповідальна за використання персональних даних, повинна дотримуватися суворих правил, які називаються "принципами захисту даних". Вони повинні переконатися, що інформація: справедливо, законно і прозоро використовується для визначених, явних цілей; зберігається не довше, ніж це необхідно; обробляється таким чином, що забезпечує відповідну безпеку, включаючи захист від незаконної або несанкціонованої обробки, доступу, втрати, знищення або пошкодження. Водночас Великобританія схвалила Стратегію кібербезпеки, яка визначає суттєвий набір цілей та показників, які відображаються у трьох важливих стовпах [29, С. 805]:

1. Захист: Уряд зміцнить власні засоби захисту інформації та працюватиме з промисловістю, щоб забезпечити захист британських мереж, даних і систем від кіберзагроз.

2. Утримання: Велика Британія зміцнить спроможність правоохоронних органів збільшити вартість кіберзлочинності.

3. Розвиток: Уряд допоможе розвивати критичні можливості Великобританії, включаючи кібер-навички, а також зростаючу індустрію кібербезпеки країни, щоб не відставати від кіберзагроз [29, С. 806].

Цифрова програма 2025 для Естонії передбачає використання ІКТ у різних сферах життя. Кінцевою метою є збільшення економічної конкурентоспроможності, добробуту людей та ефективності державного управління. Стратегія визначає різні заходи та дії для досягнення цієї мети, зокрема завершення роботи широкосмугової мережі; у майбутньому електронні послуги стануть все більш транскордонними; 20% активного населення Європейського Союзу має користуватися цифровими технологіями; Естонія почне надавати свої безпечні послуги громадянам інших країн; сприяння репутації Естонії як центру інновацій та розвитку інформаційного суспільства [29, С. 809].

Інформаційна політика Франції є складовою державної стратегії розвитку країни, стратегії франкофонії та збереження національної самобутності й ідентичності, компонентом зовнішньої політики, участі Франції в інформаційних програмах і проектах міжурядових європейських організацій, створення інформаційної економіки та поширення комп’ютерних мереж і систем, інформаційних полуг [29, С. 807].

Французька національна стратегія кібербезпеки передбачає такі стратегічні цілі: стати кіберохороною державою у кіберзахисті; забезпечити здатність Франції приймати рішення шляхом захисту інформації, пов'язаної з її суверенітетом; посилити кібербезпеку національних інфраструктур; забезпечити безпеку в кіберпросторі. Для досягнення цих цілей було визначено сім сфер діяльності [29, С. 808]:

1. Ефективно передбачати та аналізувати навколишнє середовище, щоб прийняти відповідні рішення.

2. Виявляти та блокувати атаки, оповіщення та підтримку потенційних жертв.

3. Посилити наукові, технічні, промислові і людські можливості для підтримки незалежності країни.

4. Захистити інформаційні системи держави та операторів для забезпечення кращої національної стійкості.

5. Адаптувати французьке законодавство до врахування технологічних розробок і нових практик.

6. Розробити ініціативи міжнародної співпраці у сфері інформаційної системи безпеки, кіберзахисту і боротьби з кіберзлочинністю з метою кращого захисту національних інформаційних систем.

7. Спілкуватися, інформувати та переконувати, щоб збільшити розуміння населення масштабів викликів, пов'язаних з інформаційними системами безпеки.

Головним принципом інформаційної безпеки в Німеччині є той факт, що будь-яке використання інформації заборонено. Таким чином, заборонені зберігання, передача чи зміна інформації. Це правило не поширюється лише на те використання інформації, яке дозволене законом або зацікавленою стороною.Стратегія забезпечення кібернетичної безпеки ФРН зосереджується на десяти стратегічних напрямках: захист критично важливих інформаційних інфраструктур; захист ІТ-систем в Німеччині; посилення інформаційної безпеки в державному управлінні; створення національного центру кіберреакції; утворення національної ради з кібербезпеки; проведення ефективного контролю за злочинністю у кіберпросторі; проведення ефективних скоординованих дій для забезпечення кібербезпеки в Європі і в усьому світі; використання надійних інформаційних технологій; розвиток персоналу у федеральних органах влади; інструменти для реагування на кібератаки [30, С. 66].

Національна стратегія кібербезпеки є стратегічним документом, що надає іспанському уряду основу для розробки положень Стратегії

національної безпеки з метою забезпечення запобігання кіберзагроз, захисту, виявлення, реагування та відновлення інформаційного протору. Стратегія складається з п'яти розділів. Перший «Кіберпростір і його безпека», окреслює характеристики, які визначає кіберпростір. Цей розділ показує, як особливі характеристики, які є спільними для кіберзагроз призводять до збільшення ризиків, які можуть мати серйозний вплив на національну безпеку. Другий розділ стосується мети та керівних принципів кібербезпеки в Іспанії. У третій главі Стратегія більш детально розглядає цілі кібербезпеки. Четвертий розділ визначає дії, спрямовані на забезпечення національної кібербезпеки. П'ятий розділ присвячений питанням кібербезпеки в системі національної безпеки і встановлює організаційну структуру служби кібербезпеки [31, С. 318].

При Виробленні основних положень інформаційної політики уряд Республіки Італія визначив пріоритетами трансформацію органів державного урядування на основі інформаційно-комунікаційних технологій, вільний доступ для громадян і підприємців, реалізацію електронної освіти для державних службовців, прозорість державного документообігу за допомогою Інтернету, забезпечення якості інформаційних продуктів і послуг. Виконання поставлених цілей контролюється Національним центром з питань інформатики при Державній адміністрації [32, С. 134].

У 2013 році Італія прийняла свою національну стратегію кібербезпеки. Завданнями національної стратегії є [32, С. 136]:

1. Підвищення технічного, оперативного та аналітичного досвіду всіх зацікавлених сторін та установ шляхом спільних зусиль та узгодженого підходу.
2. Зміцнення потенціалу для захисту критично важливих національних інфраструктур та стратегічних активів та зацікавлених сторін.
3. Сприяння та заохочення культури кібербезпеки.
4. Посилення можливостей протидії онлайн-злочинної діяльності, шкідливої та незаконної діяльності.
5. Посилення міжнародного співробітництва.

Крім цього, в Італії ухвалено Національний план із захисту кіберпростору та безпеки інформаційно-комунікаційних технологій. Цей Національний план визначає оперативні керівні принципи, цілі до яких переслідувати та напрямки дій, які необхідно здійснити, щоб забезпечити повну реалізацію до національної стратегії безпеки кіберпростору [32, С. 137].

Польські політичні еліти давно зрозуміли важливість побудови міцної системи кіберзахисту і перейшли до дій. В останні роки Польща демонструє послідовну державну політику боротьби із кіберзагрозами. Польща усвідомила небезпеку кіберзагроз після масштабних кібератак 2012 року. Тоді була паралізована робота урядових сайтів, а масові протести, що почалися на вулицях, прокотилися і в мережі шляхом масованих кібератак. Через це, Польща о ухвалила зміни до законодавства, які дозволяють запроваджувати у країні надзвичайний стан в разі атаки у віртуальному просторі [33, С. 110].

Сьогодні Польща спрямовує свої зусилля на безпеку та надійнійність ІКТ та побоюється зловживань та порушень - і в той же час визнає необхідність захисту відкритості та свободи Інтернету. Визначення Стратегії кібербезпеки включає наступне: «Кібербезпека повинна бути вільною від небезпек або збитків, спричинених порушенням або випаданням ІКТ або зловживанням ІКТ. Вони можуть включати обмеження доступності та надійності ІКТ, порушення конфіденційності інформації, що зберігається в ІКТ, або пошкодження цілісності цієї інформації.» [33, С. 111].

Аналіз та узагальнення міжнародного досвіду щодо формування та реалізації механізмів забезпечення державної політики інформаційної безпеки дав змогу розробити пріоритетні напрямки розвитку відповідних національних механізмів в Україні, а саме: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів в національних інтересах; створення загальної системи охорони даних; сприяння міжнародній взаємодії у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури.

РОЗДІЛ 2

СУЧАСНИЙ СТАН ДЕРЖАВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В УКРАЇНІ

2.1. Практика застосування механізмів публічного управління обміном інформацією щодо кібератак, кіберінцедентів та інцидентів безпеки інформації

Розглядаючи проблему інформаційної безпеки, важливо виділити загрози для інформаційної безпеки та проаналізувати шляхи захисту від цих небезпек. Загрози інформаційній безпеці – явища, дії факторів, що мають негативний характер або процеси, що зумовлюють: часткове або повне втрачання можливості забезпечити власні інтереси в межах інформаційної сфери соціальними об’єктами, що підлягають інформаційній безпеці; порушення нормальної життєдіяльності, здійснення руйнації або стримування розвитку об’єктів технічного інформаційного спрямування у сфері безпеки.

Закон України «Про національну безпеку України» визначає наступні загрози національним інтересам і національній безпеці України в інформаційній сфері: протиправні збирання та використання інформації; порушення технології обробки інформації; впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби; розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації; знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку; вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації; компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах; впровадження електронних пристроїв для перехоплення інформації в

технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності; знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації; перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації; використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення й розвитку української інформаційної інфраструктури; несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації [17].

З метою захисту приватної інформації в Україні був імлементований GDPR – 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. Пунктом 49 Преамбули встановлюється норма, відповідно до якої опрацювання персональних даних мірою, що є надзвичайно необхідною та пропорційною цілям забезпечення мережевої та інформаційної безпеки, тобто здатності мережі чи інформаційної системи чинити опір, на певному рівні довіри, випадковим подіям або незаконним чи зловмисним діям, що ставлять під загрозу наявність, автентичність, цілісність та конфіденційність збережених або переданих персональних даних, і безпеки пов’язаних послуг, які пропонують через такі мережі чи системи або надають за їхньою допомогою доступ органи публічної влади, групи з реагування на надзвичайні ситуації в комп’ютерній сфері, провайдери електронних послуг зв’язку та провайдери послуг у сфері безпеки, становить законний інтерес відповідного контролера даних [34].

Це може включати запобігання несанкціонованому доступу до електронних мереж зв’язку і розподіл шкідливого коду, припинення атак на «відмову в обслуговуванні», а також пошкодження комп’ютера та систем

електронного зв’язку. Для всіх секторів бізнесу обов'язок повідомляти про порушення персональних даних стає обов'язковим. Про порушення персональних даних необхідно повідомляти компетентному національному органу без зайвих затримок і протягом 24 годин. Пунктом 12 та 28 Преамбули встановлено вимоги до інформування про кіберінциденти, які охоплюють наступні елементи: від піблічної політики, ефективність якої безпосередньо впливає на реакцію суспільства, до змісту формалізованого повідомлення про кіберінцидент, швидкість надання якого впряму впливає на впровадження ефективних заходів протидії, нейтралізації та мінімізації негативних наслідків, можливості найскорішого відновлення об’єкта, на який інцидент мав негативний вплив [34].

Відповідно до стадій життєвого циклу кіберінцидент (рис. 2.1) основна частина і важливість роботи з інформування припадає саме на фазу ідентифікації. Ступінь нормативного врегулювання такого інформування впливає, з одного боку, на готовність потенційного об’єкта атаки надати інформацію про кіберінцидент до команди реагування, реалізувати план реагування, уникнути негативного розвитку наслідків кіберінциденту, вжити відповідних реагувальних заходів [34].

Рис. 2.1. Життєвий цикл кіберінциденту

У зв’язку з цим в нормативних документах у сфері кібербезпеки вчасне відповідне інформування про кіберінцидент за встановленими правилами є визначальним фактором успішності у його нейтралізації та повернення до

штатного режиму функціонування постраждалого або готовності до ефективної протидії потенційного постраждалого [35]. Схема, наведена на рис. 2.2, дає змогу визначити важливість вчасного інформування про кіберінцидент, оскільки час реагування та подальші рамки його нейтралізації можуть бути невиправданно довготривалими, що вплине на відновлення подальшого функціонування об'єкта, щодо якого мав місце кіберінцидент.

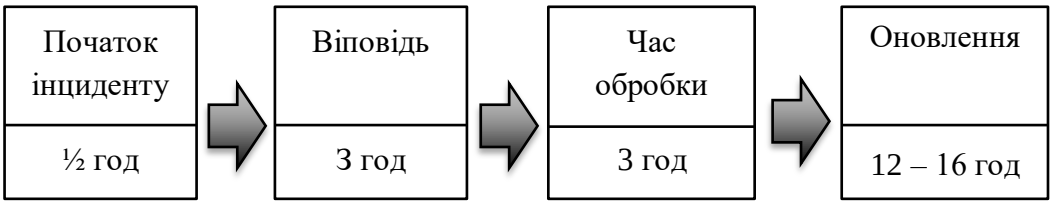


Рис. 2.2. Приклад рамок для опрацювання кіберінциденту

Узагальнений алгоритм роботи з інформацією про кіберінцедент наведено на рис.2.3.

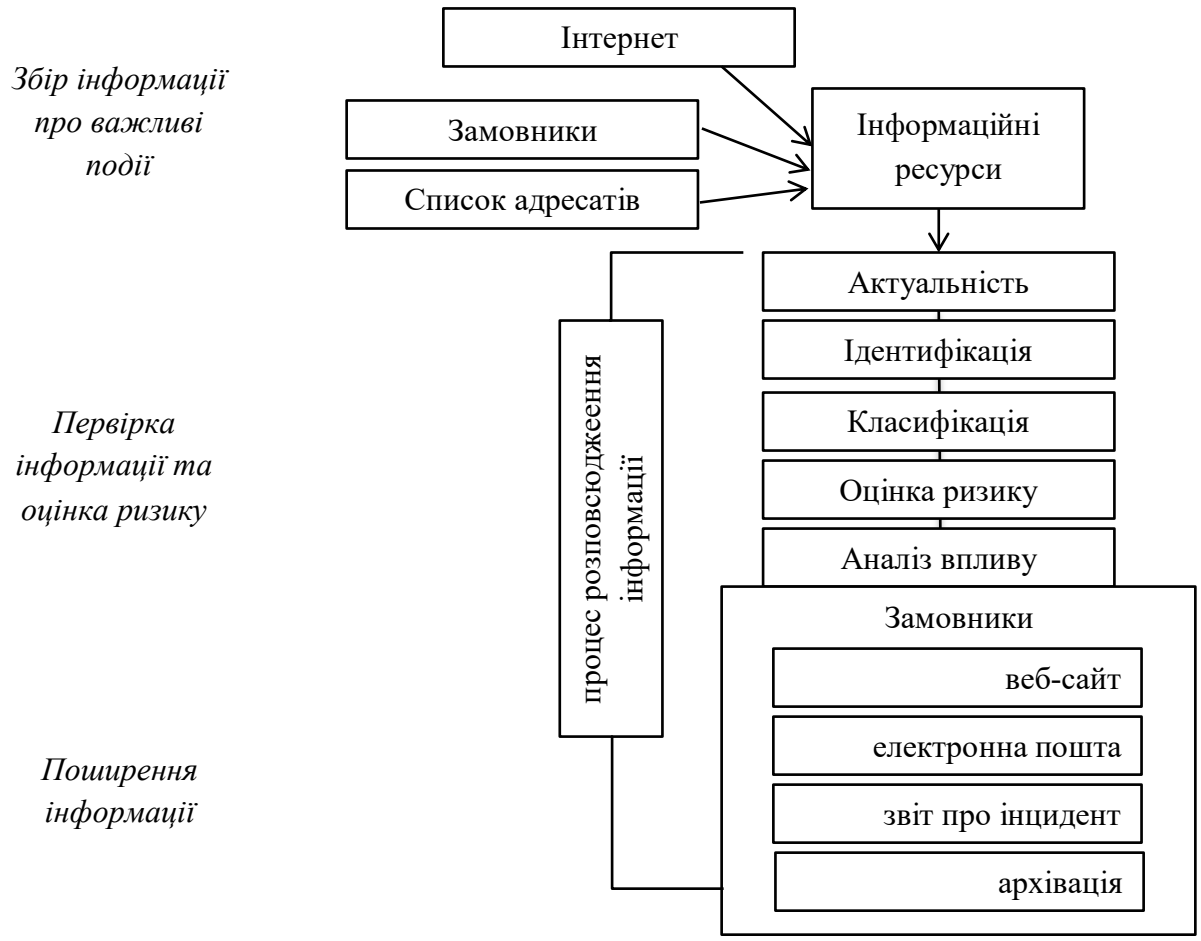


Рис. 2.3. Приклад схеми алгоримту роботи з інформацією про кіберінцидент

На основі оцінки виявленого кіберінциденту заповнюється бюлетень безпеки про оцінку ризику за наступними критеріями (рис.2.4).

Назва бюлетеня	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
№ бюлетеня	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Уражені системи:	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Назви та версія операційної системи	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
	_ _ _ _ _ _ _ _ _ _ _ _ _ _	Високий/середній/низьки
	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Ризик	_ _ _ _ _ _ _ _ _ _ _ _ _ _	Високий/середній/низьки
Наслідки/потенційні	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Зовнішні ідентифікатори	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Огляд вразливості	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Наслідки	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Рішення	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Опис	_ _ _ _ _ _ _ _ _ _ _ _ _ _	
Застосунки	_ _ _ _ _ _ _ _ _ _ _ _ _ _	

Рис. 2.4. Приклад форми інформаціного повідомлення про кіберінцидент

На рисунку 2.5 наведено приклади, які підкреслюють важливість змістовної частини інформаційного повідомлення, метою якого є надання саме необхідної інформації для опрацювання кіберінциденту.

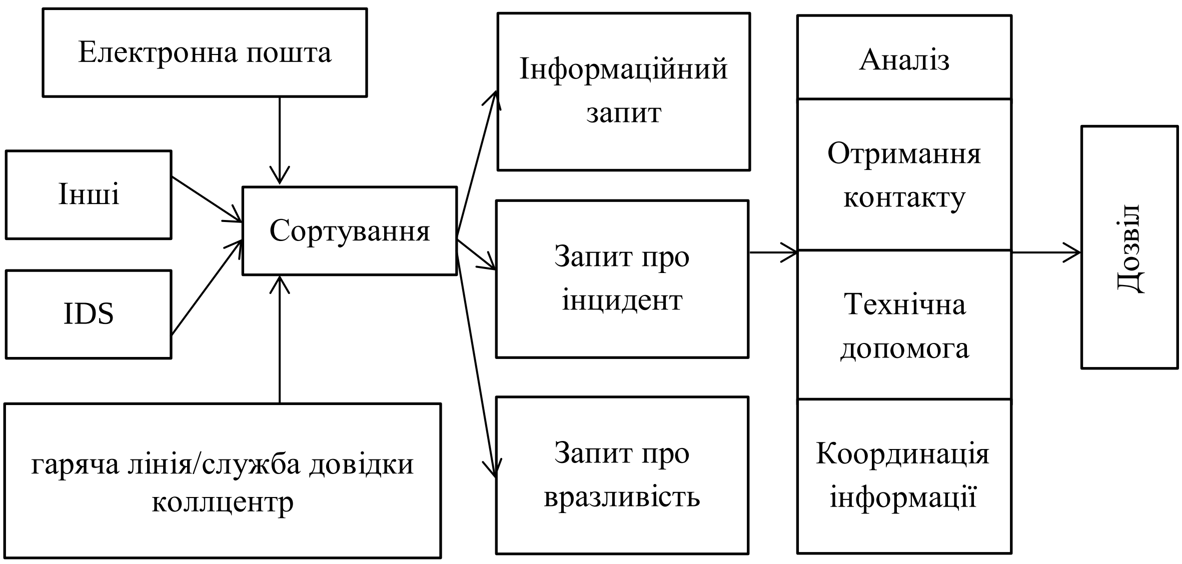


Рис. 2.5. Алгоритм та джерела отримання інформації про кіберінцидент

Особливо слід наголосити на тому, що оброблення кібепрінциденту вказані як три джерела отримання інформації про кіберінцидент, які слід розглядати як взаємно дублюючими задля забезпечення інформування на випадок відсутності можливості застосовувати елетронну пошту, платформу центру оброблення телефонних звернень або факсимільне або інший спосіб повідомлення. Зазвичай команди реагування мають працювати постійно (щоденно в режимі 24/7) і мати на це відповідні спроможності [36].

Законом ОЗКБ обмін інформацією щодо кібератак та кіберінцидентів, потенційних та реалізованих кіберзагроз є завданням суб'єктів забезпечення кібербезпеки (стаття 5), він є одним із принципів забезпечення кібербезпеки у державно-приватному партнерстві (стаття 7), одним з шляхів функціонування національної системи кібербезпеки (п. 3 статті 8), а також одним із шляхів державно-приватної взаємодії у сфері кібербезпеки (стаття 10) [15].

В Стратегії кібербезпеки України зазначено, що недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки є один із чинників, який актуалізує загрози кібербезпеці, розроблення та запровадження механізму обміну інформацією стосовно загроз критичній інформаційній інфраструктурі є одним із заходів кіберзахисту критичної інфраструктури, а розроблення та впровадження протоколів спільних дій, зокрема інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів є одним із заходів розвитку потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки [22].

В Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури [23] питання обміну інформацією про кібератаки та кіберінциденти не розглядається взагалі. На сьогодні обмін інформацією під час вжиття заходів реагування на кіберінциденти та кібератаки можливий, хоча він є обов'язковим лише щодо державних інформаційних ресурсів (ДІР – далі) із застосуванням Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств,

установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [23].

Згідно з цим порядком зазначені суб'єкти у разі виявлення спроби вчинення та/або вчинення несанкціонованих дій (доступ або спроба такого доступу без відповідно оформленого власником або уповноваженою ним особою дозволу, вірусне ураження, інші дії, які можуть призвести до порушення цілісності, доступності та конфіденційності) по відношенню до інформаційно-телекомунікаційних систем (ІТС – далі), повинні вжити заходи щодо невідкладного інформування Держспецзв'язку шляхом надсилання відповідного електронного повідомлення за встановленою цим Порядком формою. У складі Держспецзв'язку уповноважений підрозділ здійснює функції координатора, який протягом доби має бути поінформований адміністратором безпеки ІТС, щодо якої виявлені спроби або вчиненні несанкціоновані дії. Функції Держспецзв'язку як органу із забезпечення формування та реалізації державної політики кібербезпеки наведено в Додатку В. При цьому власники/розпорядники ІТС мають вжити заходів щодо фіксації ознак несанкціонованих дій та виконання, рекомендацій координатора, а також фізичний доступ його представників до ІТС для виконання заходів щодо блокування та локалізації негативних наслідків несанкціонованих дій та відновлення працездатності [37].

Координатор (у даному порядку – це команда реагування на інциденти комп'ютерної безпеки) взаємодіє, в тому числі, здійснює обмін інформацією з використанням електронної пошти, з власниками/розпорядниками ІТС, провайдерами та операторами телекомунікацій, правоохоронними органами та здійснює міжнародне співробітництво з питань, що належать до компетенції Держспецзв'язку [37].

Адміністрацією Держспецзв'язку на офіційному сайті у червні 2020 року опублікований проект Протоколу спільних дій основних суб'єктів

забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури та під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їхніх наслідків. В обґрунтуванні до його розроблення, зазначено про невідповідність вказаного Порядку координації діяльності вимогам Стратегії кібербезпеки та не поширення його норм на кіберінциденти, які не пов'язані з несанкціонованими діями щодо державних інформаційних ресурсів. Цей протокол поширюватиметься на основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак і кіберінцидентів та усунення їхніх наслідків. Особливості взаємодії основних суб'єктів забезпечення кібербезпеки в умовах особливого періоду, правового режиму воєнного та надзвичайного стану, а також в районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії та проведення антитерористичної операції визначається спільними наказами основних суб'єктів забезпечення кібербезпеки [38].

В розпорядчій частині проекту постанови визначено завдання суб'єктам взаємодії щодо визначення (створення/організації створення) підрозділів (команд, центрів, груп), які забезпечуватимуть кіберзахист та реагування на кіберзагрози щодо об'єктів критичної інформаційної інфраструктури у відповідній галузі або сфері діяльності, та/або покласти функції з кіберзахисту на підрозділи із захисту інформації [22].

Питання кібербезпеки, взагалі, та взаємодії у випадку кіберінцидентів та кібератак в банківській системі України, зокрема, визначаються Національним банком України. На сьогодні питання забезпечення кібербезпеки врегульовані постановою Правління Національного Банку України від 28 вересня 2017 року № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [39].

Так, одними із зобов’язань банків є упровадження процесу управління інцидентами безпеки інформації та розробити і затвердити документи, які містять описи дій стосовно наведених на рис. 2.6 подій.

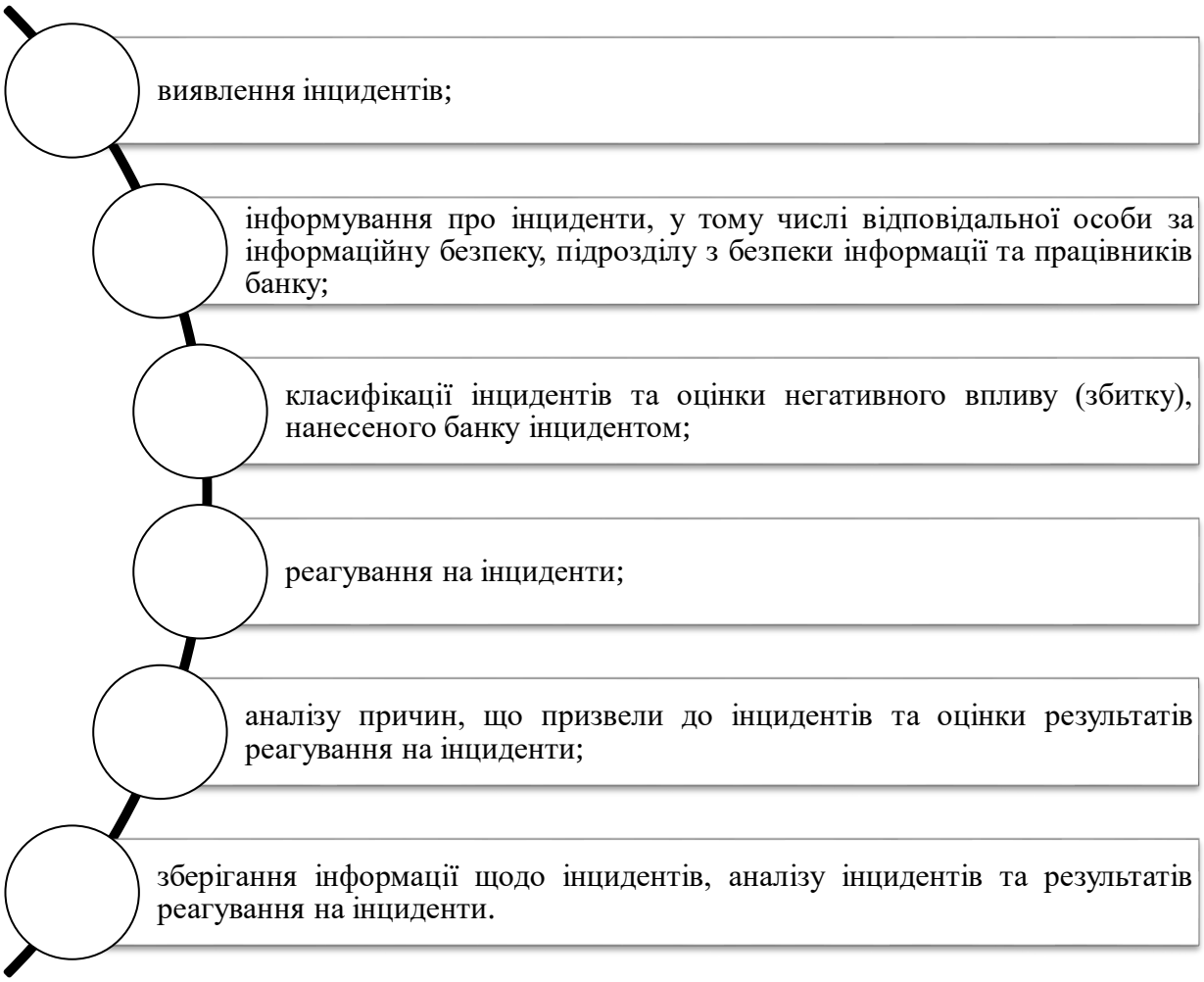


Рис.2.6. Елемнти процесу управління інцидентами безпеки інформації [22; 34 – 35]

Визначено, що у разі виявлення кіберінцидентів та кібератак, що можуть становити загрозу національній безпеці або обороноздатності держави, Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України у встановленому порядку інформує Національний координаційний центр кібербезпеки, а також надає необхідну інформацію з Державного реєстру об’єктів критичної інфраструктури, для формування Стратегії кібербезпеки України та інших стратегічних рішень в цій сфері.

2.2. Аналіз роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 – 2023 років

В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Поліпшення кібербезпекових спроможностей України в умовах воєнного стану набуло особливої актуальності, обумовленої проблемами зростання кількості та рівням кіберзагроз та кіберінцендентів в кіберпросторі внаслідок гібридної війни, яку веде Російська Федерація проти нашої держави. Лише 1 місяць 2023 року сталося 2,7 більше хакерських атак різного виду, ніж за аналогічний період 2021 року.

Ключову роль у захисті вітчизняного цифрового простору та баз даних, особливо об'єктів критичної інфраструктури, посідає підсистема оперативного центру реагування на кіберінциденти, є Система виявлення вразливостей і реагування на кіберінциденти і кіберзагрози – це сукупність програмних та програмно-апаратних засобів Держспецзв'язку, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування [35].

Зазначена сукупність програмних та програмно-апаратних засобів проводить: централізоване управління усіма підсистемами системи виявлення вразливостей і реагування кіберінциденти, кібератаки та мережеві аномалії на об'єктах кіберзахисту шляхом аналізу даних, отриманих з технічних пристроїв; централізований збір та накопичення інформації про мережеві події інформаційної безпеки; проведення моніторингу та оброблення в режимі реального часу кіберзагроз та кіберінцидентів [35].

Так, у ІІІ кварталі 2023 за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій. Кількість зареєстрованих та опрацьованих кіберінцидентів

зросла – від 64 до 115. Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програм-вайперів [40].

У III кварталі 2023 року ми зафіксували істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних. Порівняно зі статистичними даними за II квартал 2023 року кількість подій ІБ з високим рівнем критичності зросла у 3,8 разів. Відповідно, кількість зареєстрованих кіберінцидентів з високим рівнем критичності зросла на 128% [40].

Порівняно з I та II кварталами, у III кварталі 2023 року кількість критичних подій ІБ, джерелом яких є IP-адреси Російської Федерації, зросла у 35 разів. Також, порівняно з II кварталом 2023 року, майже вдвічі зросла кількість детектованих подій ІБ, пов'язаних із активним скануванням, джерелом яких є IP-адреси Росії. Саме з цих IP здійснювали кібератаки на українські інформаційні ресурси, розповсюджували фейкову інформацію, що стосується дискредитації державних органів під час російсько-української війни. Наразі найбільша кількість критичних подій ІБ пов'язана з IP-адресами зі Сполучених Штатів Америки. Проте автоматично визначена геолокація IP-адрес джерел необов'язково означає атрибуцію кібератак до ідентифікованого місцерозташування. Втім, за атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупуваннями, що фінансуються урядом рф. Зокрема, це UAC-0010 (Gamaredon) та інші [40].

Загальна кількість критичних подій ІБ зросла на 3,7%. Серед них кількість подій, автоматично визначена геолокація джерел яких асоційована з росією, збільшилась на 26%. Протягом 2023 року було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2022 році [40].

Протягом IV кварталу 2023 року за допомогою засобів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було здійсно наступну кількість заходів, наведених на рис. 2.7.

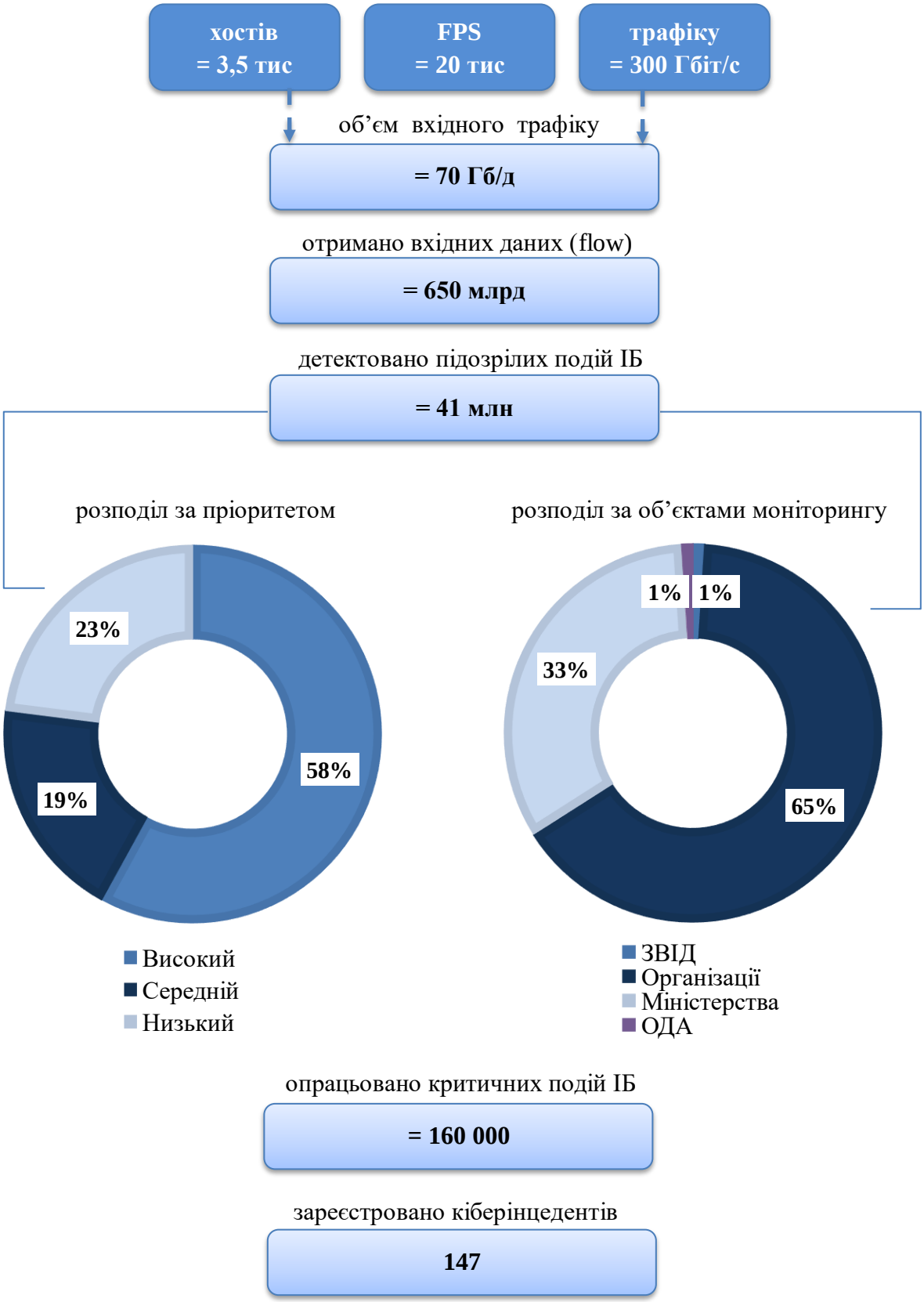


Рис.2.7. Кількість зібраних та опрацьованих даних

Опрацьовано 9 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про

кіберінциденти та кібератаки; детектовано 7 мільйонів підозрілих подій інформаційної безпеки (при первинному аналізі); опрацьовано 34 тисячі критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ і вторинного аналізу).

З початку 2023 року , порівняно з IV кварталом 2022 року, зафіксовано зменшення загальної кількості кібератак, проте їх систематичність та інтенсивність продовжує залишатись на високому рівні [40].

Але, зважаючи на посилення інформаційних операцій щодо виправдання неспровокованого вторгнення в Україну і, таким чином, створення умов для затяжної війни в Україні, немає фундаментальних підстав вважати, що тренд до зменшення кількості кібератак, націлених на українські організації різних форм власності та галузей, буде зберігатись і надалі. Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програм-вайперів (рис.2.8).

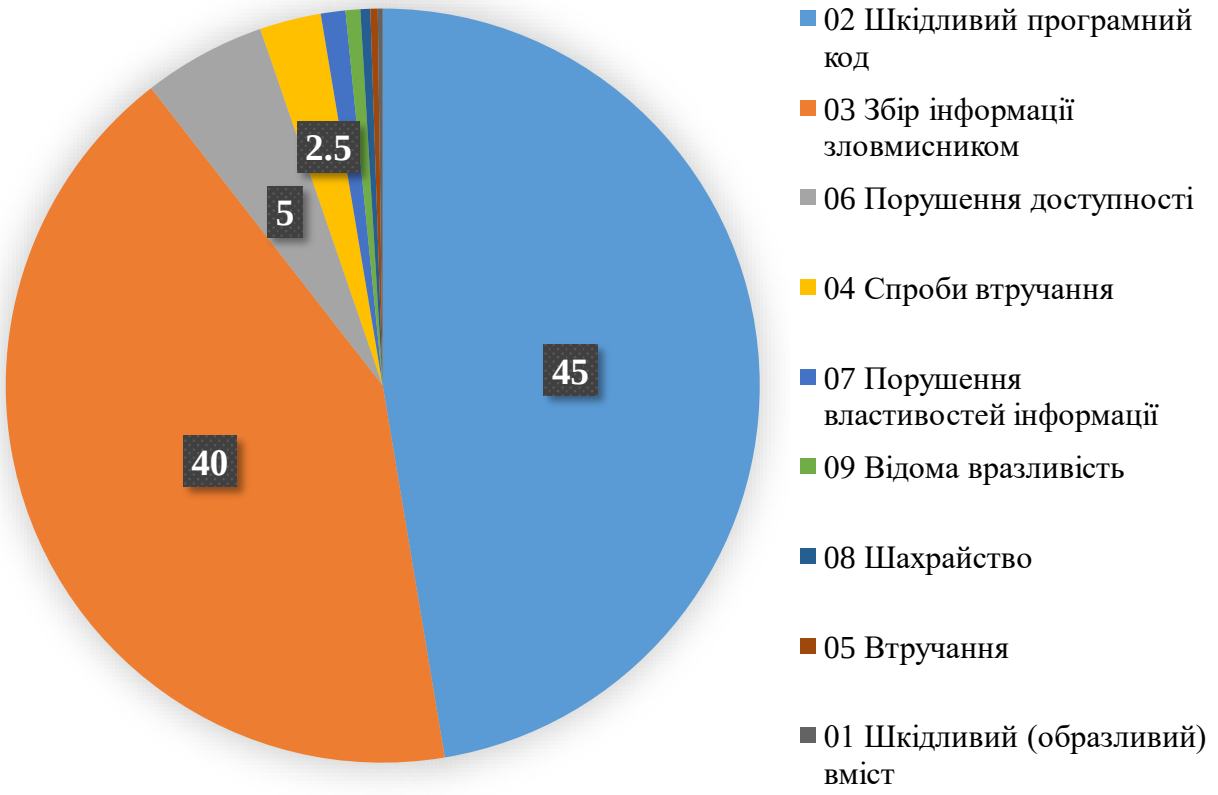


Рис.2.8. Категорії подій інформаційної безпеки

У III кварталі 2023 року зафіксовано істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних. Порівняно зі статистичними даними за II квартал 2022 року, кількість подій ІБ з високим рівнем критичності зросла у 3,8 разів [40]. Відповідно, кількість зареєстрованих кіберінцидентів з високим рівнем критичності зросла на 128% (рис.2.9).

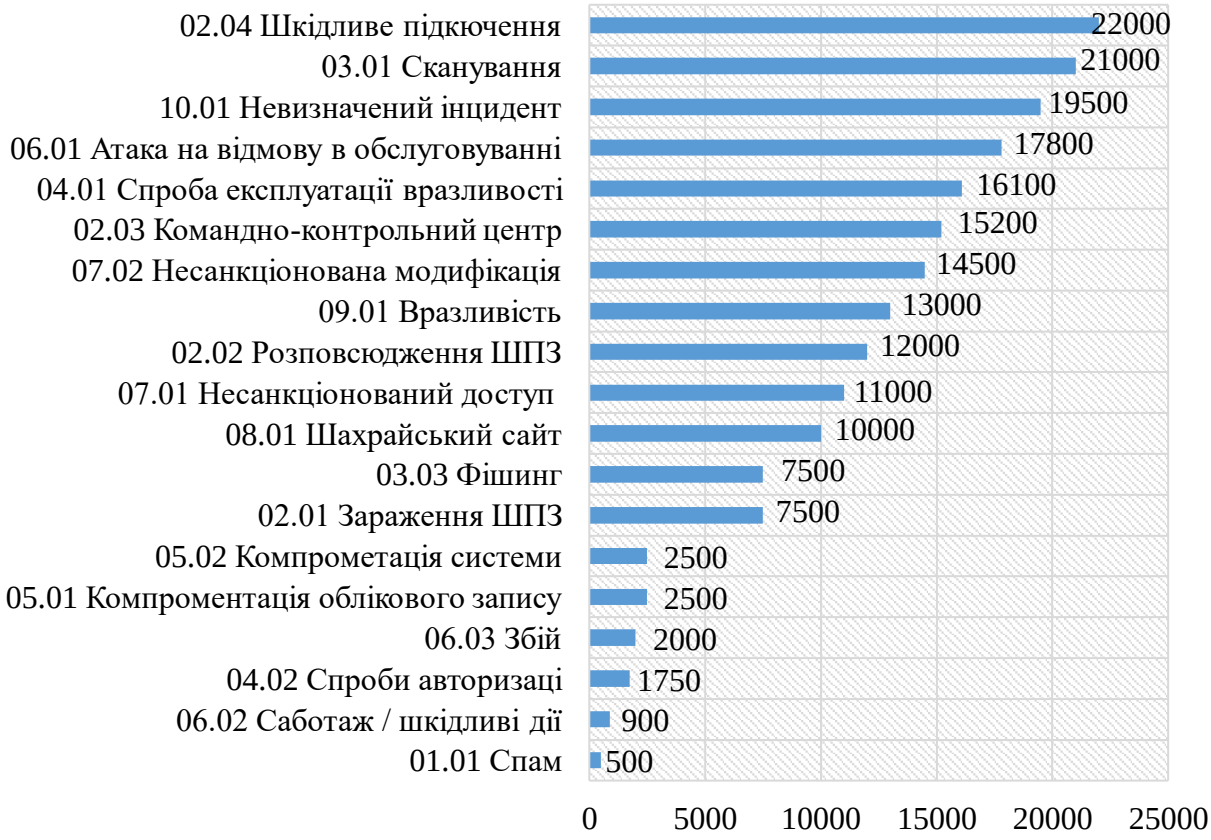


Рис.2.9. Типи подій інформаційної безпеки

43 946 підозрілих унікальних файлів було детектовано в автоматичному режимі підсистемами, що належать до складу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. BARAT, Emotet, Cobalt Strike та Meris представляють найчастіше експлуатовану C2 інфраструктуру, детектовану як джерело спроб мережевих вторгнень або порушень політик безпеки організацій, виявлених у вхідному мережевому трафіку Підсистемою збору телеметрії Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [40].

Серед сімейств шкідливого програмного забезпечення, детектованих у подіях ІБ категорії «02 Шкідливий програмний код» протягом звітного періоду, переважають Snake Keylogger, Agent Tesla, LokiBot, PurpleFox та Formbook (рис.2.10) [40].

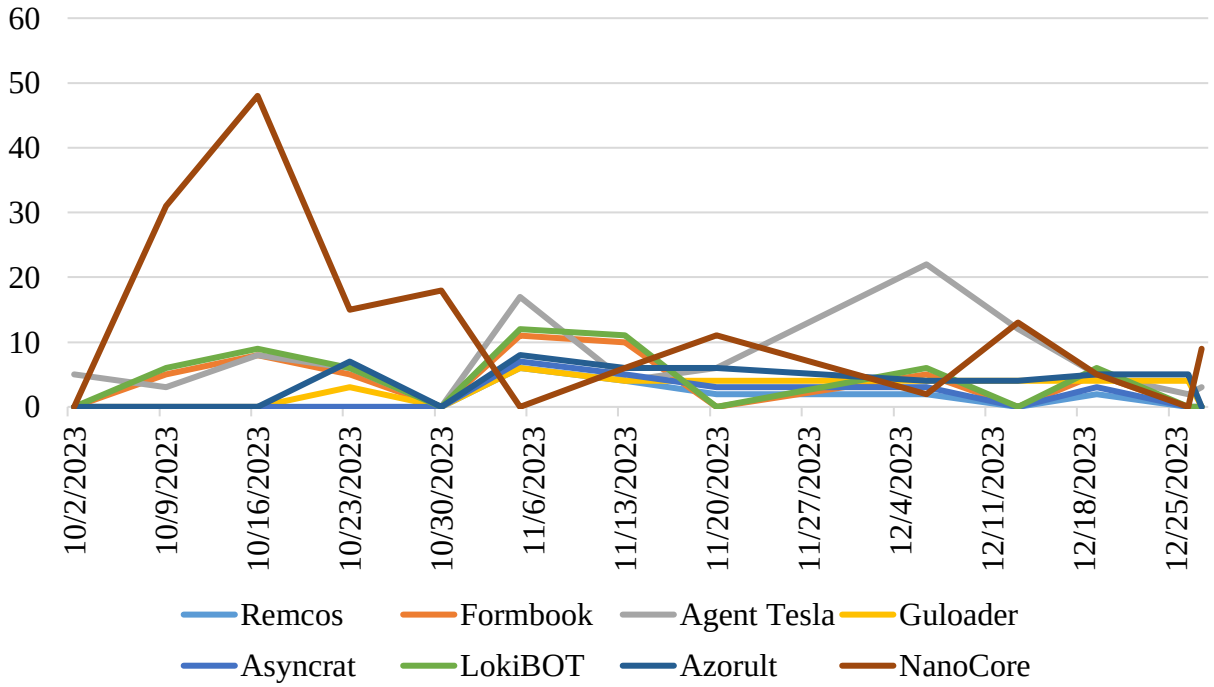


Рис. 2.10. Часовий розподіл подій інформаційної безпеки категорії категорії «02 Шкідливий програмний код»

Динаміку активності та атак проросійських хакерських угруповань за типами атак наведено на рис.2.11.

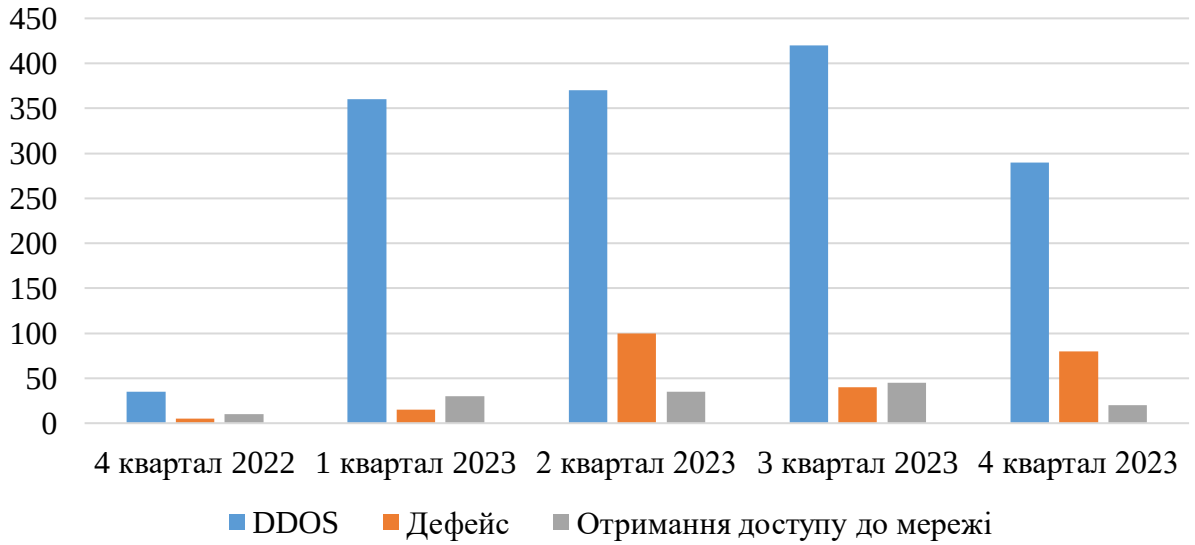


Рис.2.11. Динаміка активності та атак проросійських хакерських угруповань

Відповідно до Кібертрекеру російсько – української війни, підтримуваного користувачем, месенджер Telegram активно використовується проросійськими хактивістами як провідна платформа для організації зловмисної активності. Інтерес до платформи, як до "екосистеми кіберзлочинності", підтверджується нещодавним релізом статті Telegram - How a messenger turned into a cybercrime ecosystem by 2023 від компанії KELA, що займається кіберрозвідкою. П’ять найактивніших проросійських угруповань хактивістів, серед яких №Name057(16), RussianHackersTeam, RaHDit та Free Civillian є найактивнішими проросійськими угрупованнями хакативістів (рис.2.12). Кількість атак, організованих якими протягом I кварталу 2023 року, складає 90% від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями протягом звітного періоду [40].

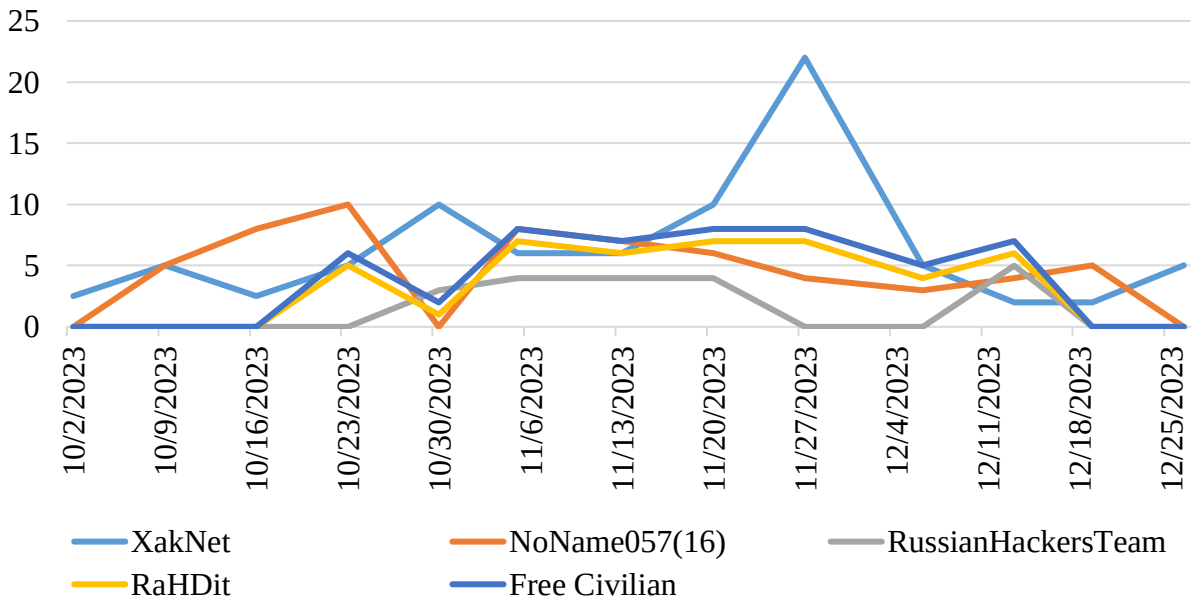


Рис.2.12. Динаміка активності проросійських хакактивістів

З початку 2023 року (порівняно з IV кварталом 2022 року) помітно (з різницею у 1,5 – 2,9 разів для різних секторів) підвищилась кількість атак, організованих проросійськими угрупованнями хакактивістів, націлених на комерційний, фінансовий сектор, уряд та місцеві органи влади, сектор безпеки та оборони. При цьому інтенсивність атак на сектор енергетики та засобів масової інформації залишається на тому ж рівні (рис.2.13).

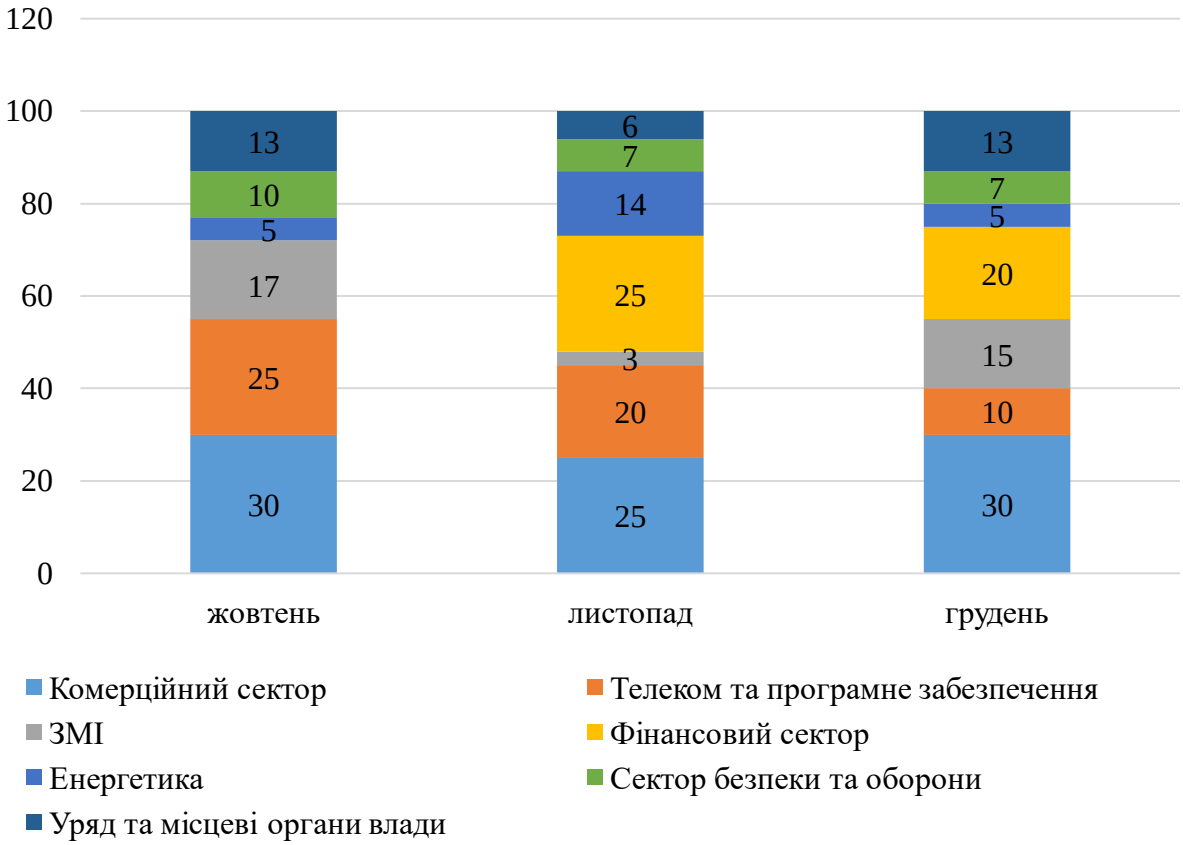


Рис.2.13. Розподіл активності хакерських угрупувань за секторами

Оскільки разом з повномасштабного вторгнення Російської Федерації на територію України активізувались ворожі хакерські групи, які безперебійно здійснюють атаки на цифрові мережі та бази даних урядових установ та бізнес – структур, захист національної кібербезпеки набув особливої актуальності. Лише 1 місяць 2023 року сталося 2,7 більше хакерських атак різного виду, ніж за аналогічний період 2021 року. Система виявлення вразливостей і реагування на кіберінциденти та кібератаки виявила 11,5 мільйонів підозрілих подій інформаційної безпеки протягом III кварталу 2023 року. Крім того, було оброблено 12 000 критичних подій інформаційної безпеки, які включали ймовірність кіберінцидентів, виявлених через вторинні аналіз і фільтрація підозрілих подій ІБ. Аналітики безпеки одночасно задокументували та обробили 355 кіберінцидентів. Кількість зареєстрованих кіберінцидентів зросла на 46% порівняно з III кварталом 2023 року. Для виявлення вразливостей та реагування на кіберінциденти та кібератаки державні, енергетичні та військові сектори підключили до 14 нових систем кіберзахисту.

2.3. Співробітництво органів публічної влади України з Європейським союзом у сфері кібербезпеки

Актуальна наразі і проблема методології захисту інформаційно-телекомунікаційного технологічного забезпечення. Сучасні загальносвітові тренди з розвитку базуються на широкому, повсюдному та динамічному впровадженні і застосуванні інформаційнокомунікативних технологій. Однак вони одночасно актуалізують проблему інформаційної безпеки та кіберзахисту (особливо для об'єктів критичної інформаційної інфраструктури), обумовлену збільшенням кількості та підвищенням складності кіберінциндентів, що посилюють ризики природного та техногенного характеру, агресією Російської Федерації, насамперед в цій сфері. З метою успішного розв'язання цієї проблеми з урахуванням міжнародного досвіду та законодавства, особливостей національного розвитку розробляється публічна політика та здійснюється публічне управління у сфері кібербезпеки [41, С. 140].

Очевидним є те, що недопрацювання в роботі інформаційної управлінської системи можуть викликати великі трагедії і величезні матеріальні збитки. Все це дає змогу для констатації, що складники інформаційної безпеки центральні для національної безпеки, особливо при входженні України до європейського простору. Безпекова сфера залишається однією із найбільш проблематичних на сьогоднішній день, особливо якщо говорити про ситуацію на сході України. Продовження бойових дій, незацікавленість сторін у проведенні відкритих переговорів та припиненні вогню, неможливість проводити відповідні дії в рамках мінських домовленостей на лінії розмежування та низка інших деструктивних явищ не сприяють подальшому розвитку відносин із ЄС.

Європою усвідомлюється те, що заходи боротьби з глобалізаційними загрозами будуть дійсно дієвими тільки при налагодженні відповідних структур обміну інформаційними даними між її учасниками. Україною

вживаються усі можливі заходи щодо євроінтеграційних державотворчих процесів. В такому разі вона невідворотно зустрінеться з проблемами по узгодженню підходів до безпеки з ЄС із забезпеченням своєї інформаційної безпеки [41, С. 142].

Цей напрям як пріоритетний формально визначено в цілій низці законодавчих актів України, що стосуються розвитку національної безпеки, інформаційного (цифрового) суспільства, цифрової економіки, європейської та євроатлантичної інтеграції України, тощо. Так, наприклад, метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, для досягнення якої, поряд з іншим, необхідними є поглиблення міжнародного співробітництва у цій сфері [22].

В щорічних планах заходів з її реалізації передбачено заходи з виконання завдання щодо розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у цій сфері та співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі в заходах зі зміцнення довіри у кіберпросторі. Однак, актуальною залишається проблема їх реального впровадження та взаємоузгодженості, прискорення імплементації сукупності міжнародних документів, насамперед ЄС та НАТО, координованості дій та взаємодії основних об’єктів та суб’єктів кібербезпеки та кіберзахисту. Окрім того, формування національної системи кібербезпеки здійснюється вкрай повільно, що не відповідає сучасній військовополітичній обстановці та соціально-економічному стану України, загрози збільшуються у тому числі через недосконаліть публічного управління та адміністрування, особливо на стратегічному рівні [42, С. 143].

При цьому як показує практика провідних країн світу в умовах суттєвої невизначеності та непередбачуваності функціонування систем публічного управління та адміністрування переваги мають насамперед методи стратегічного планування та управління.

Сама Стратегія кібербезпеки ЄС підкреслює важливість створення «на основі фактичних даних оцінювання ризиків та культури управління» всередині спільноти кібербезпеки в ЄС та залучення зацікавлених сторін у всіх її сферах. Найбільш конкретні вказівки щодо стратегій оцінювання в кібербезпеки походять з посібника з передової практики ENISA щодо формулювання стратегій. Модель життєвого циклу стратегії проілюстрована на рис.2.14 передбачає діяльність з оцінювання і стосується разових, постійних та періодичних оцінок. Так, передбачається чотири фази життєвого циклу стратегії: розроблення стратегії, виконання стратегії, оцінка стратегії та підтримка стратегії. Щодо зворотніх зв'язків, які встановлюються та впливають на кожну фазу виконання стратегії, то передбачені ними заходи визначені від четвертої до першої фази таким чином: продовження поліпшення, періодичне оцінювання стратегії, оновлення плану заходів та оновлення стратегії [43].

Рис. 2.14. Життєвий цикл національної стратегії кібербезпеки [43]

Україна приєдналась до ряду ініціатив ЄС, які посилюють її спроможність протидіяти кіберзагрозам: залучення до роботи ENISA та Європейського центру досліджень та компетенцій з кібербезпеки та тренінгів ЄС щодо координації механізмів спільного реагування ЄС та держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки.

У 2019 році за Міністерством Юстиції як координатором напрямку «Юстиція. Свобода. Безпека» в рамках поглиблення Асоціації внесено пропозиції української сторони щодо оновлення Плану дій Україна – ЄС у цій сфері захисту цифрового інформаційного середовища, а саме: виокремити в розділі «Співробітництво у сфері забезпечення кібербезпеки та захисту інформації», в якому передбачити такі основні подальші ціл [44]:

– посилити співпрацю між ЄС та органами влади України стосовно заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем, а також обміну найкращими практиками між кіберорганізаціями ЄС та України;

– розпочати переговори щодо підписання Угоди про співробітництво з ENISA між Україною та ЄС;

– розпочати співробітництво з ENISA з питань скоординованого розкриття вразливостей за досвідом країн-членів ЄС;

– подальше розширення дорадчої та технічної підтримки ЄС в сфері кібербезпеки та захисту інформації;

– підвищення рівня підтримки ЄС щодо підготовки кадрів у профільних установах України з кібербезпеки, а також сприяння розвитку співпраці у сфері інновацій в галузі кібербезпеки та захисту інформації;

– залучення правоохоронних органів України до ініціатив ЄС у сфері посилення кібербезпеки з урахуванням прийняття пакету з кібербезпеки;

– залучення України до діяльності Європейського дослідницького центру з кібербезпеки та до тренінгів ЄС стосовно координації механізмів спільного реагування держав-членів ЄС на масштабні кібератаки та кіберінциденти, а також вивчення досвіду країнчленів ЄС з питань запобігання, виявлення, припинення та розслідування кібератак та кіберінцидентів;

– створення, під егідою Комітету з кіберзлочинності Ради Європи національних робочих груп експертів з числа постійних членів проектів ЄС, представників заінтересованих державних органів та досвідчених фахівців у

сфері нормотворчості, представників наукових та бізнес-кіл, які опрацьовуватимуть та розроблятимуть пропозиції щодо вдосконалення чинного законодавства для повної імплементації положень Конвенції;

– здійснення фахової експертизи на рівні експертів ЄС проектів законодавчих актів, запропонованих за результатом роботи даних груп.

Таким чином, постійний аналіз ефективності національних стратегій є методологічним підґрунтям для їх перегляду в залежності від фази життєвого циклу таких стратегій. В Стратегії кібербезпеки України зазначено, що розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, зокрема, періодичного проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки, а поняття аналізу ефективності не згадується взагалі (рис.2.1).

Таблиця 2.1

Зіставлення стратегій кібербезпеки в ЄС та Україні [22; 43]

<table>
<tr><th>NCSS (ENISA)</th><th>Стратегія кібербезпеки України</th><th>Висновок про відповідність</th></tr>
<tr><td>Структура</td><td>Національна система кібербезпеки. Чітко окреслені держ. органи та не чітко «інші суб’єкти»</td><td>Скоріше присутній</td></tr>
<tr><td>Механізми</td><td rowspan="4">створення безпечного кіберпростору, кіберзахист інформаційного активу держави та інфраструктури його оброблення, кіберзахист критичної інфраструктури, кібероборона, боротьба з кіберзлочинністю</td><td rowspan="4">Скоріше присутній, але без обов’язків та прав суб’єктів</td></tr>
<tr><td>Заходи, ролі (завдання), обов'язки та права</td></tr>
<tr><td>Цілі та засоби розвитку національних можливостей</td></tr>
<tr><td>Визначення критичної інформаційної інфраструктури</td></tr>
<tr><td>Системний та інтегрований підхід до національного управління ризиками</td><td>періодичне проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки</td><td>Майже відсутній</td></tr>
<tr><td>Плани готовності, реагування та відновлення, заходи щодо захисту КІІ</td><td></td><td>Відсутній</td></tr>
</table>

Таким чином, моніторинг ефективності її виконання в Стратегії кібербезпеки України не передбачений і має бути відображений в її оновленому варіанті від 2026 року. Згідно Звіту про виконання Угоди про асоціацію між Україною та Європейським Союзом у 2022 році за чотирма пріоритетними напрямками інтеграції до ЄС в рамках п'ятого засідання Ради асоціації підписано п'ять міжнародних договорів про фінансування нових програм міжнародної допомоги у сфері захисту кіберпростору із загальним бюджетом у 2023 році 222,5 млн. євро. (табл. 2.2). Предметом зазначених договорів визначено реформування, у тому числі, стандартизації, електронного зв'язку, кібербезпеки та розширення контактів України та країн-членів ЄС з метою професійного обміну [45].

Таблиця 2.2

Програма міжнародної технічної допомоги з боку ЄС 2020 - 2023 роки

2020	2021	2022	2023
EU Sure 55 + 40 млн. євро	Навчальні програми кібербезпеки у вищій освіті15 млн. євро	Відділення асоціації ENISA України 13 млн. євро	Фінансування Фонду енергоефективності 50 млн. євро
U-LEAD з Європою 90 млн. євро	Підтримка цифровізації державного управління 104 млн. євро	Програма технічного співробітництва 37 млн. євро	Управлвння державними фінансами 55,5 млн. євро
Програма технічного співробітництва 15 млн. євро	Створення ситуаціних центрів в Україні 52,5 млн. євро	NIF – Local current lending 50 млн. євро	Підтримка енергоефективності в Україні 54 млн. євро
	Technical cooperation facility 25,6 млн. євро		Програма технічного співробітництва 37 млн. євро
			Програма ЄС для навичок 58 млн. євро
			Програма сприяння міждюдським контактам 18 млн. євро
200 млн. євро	200 млн. євро	100 млн. євро	272,5 млн. євро

В подальшому на основі принципів визнання важливості Стратегії кібербезпеки Європейського Союзу необхідно передбачити реалізацію заходів з підтримки прийняття стандартів, що встановлюватимуть базис для обміну інформацією про загрози та захисні заходи, а також з розроблення та впровадження рекомендацій та практик з безпеки інформації в рамках новостворюваної робочої групи з кібербезпеки визначити вимоги з кібербезпеки, пов'язані із забезпеченням захисту персональних даних у відповідності з резламентом із захисту персональних даних, електронної ідентифікації та електронних довірчих послуг, визначити загальні схеми інформаційного обміну та кооперації, взаємного визнання сертифікатів з кібербезпеки між країнами-членами ЄС, а також навчальних візитів до центрів з забезпечення безпеки в одній з країн-членів ЄС.

Як зазначалось вище, Україні на законодавчому рівні визначено необхідність та пріоритетність здійснення міжнародного співробітництва в кібербезпековій сфері з використанням організаційно-правових та фінансових механізмів міжнародного співробітництва у сфері кібербезпеки з Україною, які зіставлено з існуючими спроможностями України в цій сфері, яке вона здійснює як на двосторонній основі з окремими державами, так і з їх об'єднаннями. Аналіз практичної релізації заходів коорепації в галузі захисту цифрового середовища показав, що незважаючи цілу низку розроблених та імплементованих організаційноправових механізмів державного управління міжнародним співробітництвом, однією з головних проблем залишається проблема координованості дій суб'єктів кібербезпеки, і яка є основною причиною недостатньої ефективності державної політики в цій сфері. Виокремлено напрямки удосконалення національних механізмів державного управління на основі практики міжнародного співробітництва, які доцільно буде додати в оновлену редакцію Стратегії кібербезпеки України з метою позбавлення вад її чинної версії та містити більш конкретні завдання і заходи із забезпечення кібербезпеки з можливістю їх коригування відповідно до загроз у кіберпросторі.

РОЗДІЛ 3

НАПРЯМКИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В УКРАЇНІ

3.1. Рекомендації щодо удосконалення проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури

Динамічний розвиток та проникнення інформаційно-комунікативних технологій в усі сфери життєдіяльності громадянина, суспільства та держави актуалізує проблему забезпечення актуальності кібербезпеки та ефективності заходів кіберзахисту (особливо для об'єктів критичної інформаційної інфраструктури), обумовлену як збільшенням кількості та підвищенням складності кіберзагроз, кіберінциндентів, кібератак, насамперед з боку Російської Федерації, так і недостатньою готовністю або відповідністю сучасним вимогам національної системи кібербезпеки до ефективної їх нейтралізації та протидії, знаходиться в стадії свого активного розвитку. Успішне розв'язання цієї проблеми передбачає розробку окремої публічної політики та здійснення публічного адміністрування у сфері кібербезпеки та кіберзахисту на основі якісної та оперативної вхідної інформації – основи прийняття управлінських рішень на всіх рівнях, зокрема на стратегічному.

При цьому існують два принципово різні підходи до організації та проведення огляду стану кіберзахисту. Згідно з першим підходом передбачається розробка окремого комплексу процедур спостереження, вимірювання, аналізу та оцінювання, орієнтованих на формування та виконання загальнодержавних концептуальних, програмних та планових документів. Другий підхід орієнтовано на ефективне використання вже існуючих в системі кібербезпеки та кіберзахисту процедур, їх уточнення (за

необхідності) та раціональне об'єднання в єдину процедуру огляду стану кіберзахисту. Перший підхід потребує більших зусиль та ресурсів на його розробку та впровадження, але саме він потенційно в найбільшій ступені відповідає потребам інформаційно-аналітичного забезпечення процесам формування та реалізації публічної політики та адміністрування в цій сфері. Головною перевагою другого підходу є суттєве зменшення витрат на проведення огляду, у тому числі, часових витрат та на підготовку суб'єктів та об'єктів кіберзахисту до проведення вищевказаних процедур. Другий підхід можна також розглядати як підготовчий (попередній) етап до переходу до першого підходу. Враховуючи особливості сучасного розвитку України, насамперед щодо необхідності якомога швидшого прийняття рішень з розв'язання проблем у сфері кібербезпеки та кіберзахисту з мінімально можливими при цьому ресурсними витратами, розглянемо більш детально другий підхід до організації та проведення огляду [46].

Законодавством, що стосується національної безпеки, зокрема сфери кібербезпеки та кіберзахисту, визначено низку неугоджених між собою та нерозкритих за своїм змістом, об'єктами, суб'єктами (їх чітких функцій та завдань, взаємодії між собою) тощо інструментів отримання достовірної, точної, повної, своєчасної інформації про стан кіберзахисту. До цих інструментів, насамперед відносяться: самооцінка об'єктів критичної інфраструктури (ОКІ – далі) стану кіберзахисту їх об'єктів критичної інформаційної інфраструктури (ОКІІ – далі), що базуються, у тому числі, на застосуванні механізмів державно-приватного партнерства; зовнішні оцінки за результатами проведення державно го контролю, незалежного аудиту, негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів та інші [21]. Проблема полягає як у відсутності або неповної формалізації кожного з вищевказаних інструментів, більшість з яких знаходяться поки що тільки в стадії своєї розробки, так і в їх комплексному застосуванню з урахуванням переваг та вад кожного з них.

Саме таким комплексним об'єднуючим механізмом оцінювання стану

кіберзахисту відповідно до другого підходу, на думку авторів, повинен бути механізм державного управління «оглядом стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом", який сформульовано в статтях 22 та 27 Закону України «Про національну безпеку України» без розкриття його сутності та змісту [17].

У загальній проблемі забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури та державних інформаційних ресурсів особливо актуальною є проблема розробки та впровадження науково- методологічних підходів до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури з урахуванням міжнародного досвіду в цій сфері. Окрім того, п.4.4 Стратегії кібербезпеки України [22] та п. 3 статті 8 Закону ОЗКБ [15] передбачена процедура «періодичного проведення огляду національної системи кібербезпеки та розроблення індикаторів стану кібербезпеки» як одного з пріоритетних напрямів діяльності національної системи кібербезпеки, але без чіткого її визначення, взаємозв'язку з іншими оглядами сектору безпеки та оборони, насамперед оглядом стану кіберзахисту державних інформаційних ресурсів та крикритичної інформаційної інфраструктури, а також з комплексним оглядом сектора безпеки та оборони, що є колізією вищевказаних законодавчих актів з Законом України «Про національну безпеку України» [17].

З урахуванням міжнародного досвіду та шляхом застосування запровадженого в законі уніфікованого підходу до визначення вищенаведених оглядів у сфері національної безпеки України, пропонується таке визначення огляду стану кіберзахисту – державних інформаційних ресурсів та критичної інформаційної інфраструктури, а саме це — процедура періодичного спостереження, вимірювання, аналізу та оцінювання стану і готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем (ІТС), в яких обробляються та зберігаються державні інформаційні ресурси та інформація, вимога щодо

захисту якої встановлена законом; спостереження стану кіберзахисту – активне, систематичне, цілеспрямоване, планомірне і вивчення реального стану кіберзахисту, спрямованих на запобігання кіберінцидентам, виявлення, попередження та припинення ліквідацію їх наслідків кібератак, здатності об'єктів критичної інформаційної інфраструктури до відновлення роботи після кібератак та кіберінцидентів. Його структуру наведено в додатку Г.

Виходячи з законодавства, головну мету огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури (далі – огляд) можна сформулювати як: визначення стану захищеності і готовності державних інформаційних ресурсів та критичної інформаційної інфраструктури до запобігання кіберінцидентам, оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення, функціонування цих об'єктів і систем. Система принципів проведення огляду повинна базуватись на загальних принципах кібербезпеки, визначених в статті 7 Закону ОЗКБ, які з урахуванням його особливостей доцільно трансформувати в такі [17]:

– системного та комплексного застосування інструментів огляду з урахуванням їх специфіки, утому числі, переваг, вад, обмежень на використання, тощо кожного з них;

– координованості та забезпечення балансу між окремими видами оглядів в системі оглядів комплексного огляду сектору безпеки і оборони;

– прозорості використання ресурсів у сфері кіберзахисту;

– об'єктивності, який полягає в тому, що огляд проводиться на основі вихідних даних власників (розпорядників, операторів) об'єктів огляду, що відображають реальний стан кіберзахисту;

– результативності, який грунтується на гарантуванні державою науково-методичного, організаційно – технічного, інформаційного, матеріального та фінансового забезпечення завдань «Стратегії кібербезпеки України» та з урахуванням фінансово-економічних можливостей держави;

– обмеженої гласності, який полягає в тому, що проведення ОСК є прозорою процедурою, а результати отриманні при виконанні заходів огляду щодо конкретних механізмі кіберзахисту на об'єктах огляду до певного моменту часу є інформацією з обмеженим доступом.

Передбачається реалізація таких основних завдань [17]:

– визначення галузі (галузей) та об'єктів, щодо яких здійснюватиметься проведення ОСК;

– формування плану заходів з проведення ОСК з урахуванням їх галузевої та об'єктової специфіки;

– оцінювання затверджених власниками (розпорядниками) об'єктів огляду ризиків та відповідних ним політик інформаційної безпеки;

– наявність на об'єктах огляду систем безпеки інформації, відповідність їх створення, уведення в експлуатацію, експлуатації та модернізації вимогам міжнародних та галузевих стандартів або наявність комплексних систем захисту інформації з підтвердженою відповідністю;

– визначення на об'єктах огляду підрозділів безпеки (захисту) інформації та кіберзахисту, залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до проведення огляду, підготовки Звіту про результати його проведення та проектів концептуальних та планових документів у сфері кібербезпеки та кіберзахисту;

– впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів;

– оцінка ефективності протоколів взаємодії об'єктів огляду, команд реагування на комп'ютерні надзвичайні події (команд реагування) при кібератаках та кіберінцідентах;

– підготовка методичних та навчальних матеріалів для підвищення кваліфікації спеціалістів у сфері кіберзахисту, підготовки кадрів;

– визначення та/або вдосконалення критеріїв ризиків для заходів із здійснення державного контролю у сфері кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Відповідно до цих завдань огляд є основним інструментом інформаційно – аналітичного забезпечення формування та виконання Стратегії кібербезпеки України, завдань та проектів до Національної програми інформатизації, інших концептуальних, програмних та планових документів у сфері кібербезпеки та кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. За рішенням Ради національної безпеки і оборони України (РНБО – далі), яке вводиться в дію указом Президента України, огляд може здійснюватися як у складі комплексного огляду сектору безпеки і оборони, так і окремо, але в обох випадках саме на Уряд покладається завдання щодо визначення загального порядку його проведення, насамперед щодо організації, контролю та попереднього схвалювання результатів проведення та надання звіту у встановленому порядку на розгляд і остаточне затвердження РНБО [46, С. 42].

При цьому законодавством чітко не визначено місце і роль такого важливого огляду як «періодичне проведення огляду національної системи кібербезпеки» в комплексному огляді сектору безпеки і оборони, формуванні та реалізації Стратегії національної безпеки України, Стратегії кібербезпеки України та інших документів, а також його взаємодія з оглядом стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Водночас механізм виконання Стратегії кібербезпеки України, що передбачає щороку розробляти і затверджувати плани заходів з її реалізації та щопівроку інформувати про стан їх виконання, є декларативним, ресурсна непідтриманим, вкраї інерційним. Так, наприклад, плани заходів з реалізації Стратегії кібербезпеки України у 2022 та 2023 роках приймались з запізненням відповідно на 3 та 7 місяців, а систему індикаторів стану кібербезпеки, яка має включати в себе підсистему індикаторів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, и досі не розроблено [22].

Тому, крім вищевказаних варіантів застосування огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури (автономного та у складі комплексного огляду сектору безпеки та оборони) необхідно також передбачити його застосування у складі процедури періодичного проведення огляду національної системи кібербезпеки, який може також здійснюватися або автономно або у складі комплексного огляду сектору безпеки та оборони.

Оцінювання ефективності заходів з кіберзахисту може здійснюватись підрозділами захисту інформації/інформаційної безпеки власників розпорядників) ОКІ (самооцінювання) або, на договірних засадах, Державним центром кіберзахисту, командами реагування на надзвичайні комп'ютерні події, які відповідають встановленим для них вимогам, а також підприємствами, установами і організаціями, які мають відповідну компетенцію (ліцензію) на право провадження господарської діяльності у сфері захисту інформації, або здійснюють аудит інформаційної безпеки [17].

При цьому самооцінка заходів з кіберзахисту ОКІ є основною процедурою огляду і повинна здійснюватися постійно з урахуванням внутрішньо об'єктового режиму на підставі затверджених власниками (розпорядниками) таких об'єктів ризиків інформаційної безпеки та відповідних ним запроваджених заходів і процесів безперервності забезпечення кіберзахисту державних інформаційних ресурсів та ОКІІ, а також визначених власниками (розпорядниками) ОКІ [17]:

– об'єктів спостереження та вимірювання, включаючи процеси інформаційної безпеки та заходи безпеки;

– методики спостереження, вимірювання, аналізу та оцінювання, які можуть бути застосовані для гарантування достовірності та обґрунтованості їх результатів;

– причин, підстав та суб'єктів проведення спостереження, вимірювання, аналізу та оцінювання.

При проведенні самооцінювання або оцінювання ефективності заходів з кіберзахисту об'єкта огляду щонайменше оцінюється виконання загальних вимог забезпечення кіберзахисту, затверджених Урядом, а саме його власником (розпорядником) або суб'єктом, що здійснює аудит інформаційної безпеки, формуються відомості про запроваджені заходи з кіберзахисту.

При цьому актуальною проблемою є обгрунтований вибір системи показників вимірювання стану кіберзахисту об'єктів огляду, яка обумовлена як різнотипністю цих об'єктів, так і різноманітністю складових огляду, їх цілей, інструментів застосування та підсистем показників і індикаторів, методичних апаратів спостереження, вимірювання, аналізу та оцінювання тощо. Формування загального підходу до вимірювання (оцінювання) стану кіберзахисту для таких умов може здійснюватися наступним шляхом (рис.3.1).

Рис.3.1. Загальний підхід до вимірювання (оцінювання) стану кіберзахисту

Кожен з вищевказаних підходів має свої переваги та вади. Так найменш витратним є перший підхід, реалізація якого окрім того потребує й найменших зусиль. Але просте об'єднання існуючих підсистем вимірювання (оцінювання) стану кіберзахисту об'єктів огляду може не в повній мірі відповідати вимогам ефективного формування та виконання, наприклад, Стратегії кібербезпеки України, оскільки досягнення часткових цілей складових огляду зовсім не означає досягнення його загальної цілі.

Формування системи показників (індикаторів) на основі однієї з міжнародних систем показників з адаптацією її до мети та завданьнаціональної політики у сфері кіберзахисту, а також розподіл її показників між показниками складових огляду або без такого розподілу є достатньо раціональним з точки зору розв'язання зазначеної проблеми. При формуванні системи показників необхідно врахувати той факт, що частина з них має якісний характер, а кількісні показники — різні шкали вимірювань, що суттєво ускладнює процедуру оцінювання. Тому одним з головних завдань Держспецзв'язку має бути розроблення типової методики спостереження, вимірювання, аналізу та оцінювання, які можуть бути застосовані для гарантування достовірності та обгрунтованості їх результатів.

Узагальнюючи напрямки вдосконалення публічного управління задля підвищення ефективності забезпечення кібербезпеки України, можна виділити наступні: впровадження механізмів встановлення відповідності змісту щорічних заходів з реалізації Стратегії кібербезпеки України її цілям, осучаснення принципів планування та контролю за виконанням цих заходів; розширення кола суб’єктів-учасників виконання щорічних планів заходів з реалізації заходів кібербезпеки України. Необхідно також доповнити положення щодо запровадження сучасних механізмів стратегічного планування завданнями з формування переліку та планів забезпечення стійкості об’єктів критичної інформаційної інфраструктури, впровадження системного та інтегрованого підходу до управління ризиками кібербезпеці на національному рівні, що сприятиме підвищенню її результативності.

3.2. Пропозиції щодо внесення змін до законодавчих актів із підвищення рівня кібербезпеки та інформатизації

Основним (базовим) законом у сфері кібербезпеки є Закон ОЗКБ. Проте сфреа кібербезпеки невід'ємно пов'язана з іншими сферами, а саме: національної безпеки, захисту інформації, інформатизації, телекомунікаційною, банківською, енергетичною, транспортною та іншими сферами критичної інфраструкутури та критичної інформаційної інфраструктури [15]. Напрямками вдосконалення нормативно – правового забезпечення кібезрбезпеки держави можуть бути:

1. Корекція термінології у сфері кібербезпеки в бік відповідності визначень міжнародним практикам: відкоригувати існуючі та увести нові терміни: «кібербезпека – захищеність інформації в кіберпросторі» та «індикатор кіберзагроз» – інформація, необхідна для виявлення, опису або ідентифікації (рис.3.2).

Рис.3.2. Визначення поняття «індикатор кіберзагроз»

2. Впровадити перелік подій, які при визначенні їх як кіберінциденти мають обов'язково оброблятися відповідно до встановлених правил, у тому числі щодо звітування про результати їх оброблення.

3. Встановити основні принципи планування, бюджетування, виконання та аналізу ефективності заходів з виконання Стратегії кібербезпеки України, при цьому встановити, що всі суб'єкти забезпечення кібербезпеки можуть брати участь у цих заходах, пройшовши акредитацію, якщо вони не основні елементи національної системи кібербезпеки.

4. Запровадити галузевий принцип формування переліку ОКІ та ОКІІ та встановлення галузевими регуляторами правил та норм забезпечення дотримання принципів кібербезпеки в галузях, якими вони опікуються.

5. Поширити сферу дії Закону на діяльність, пов'язану з обробленням інформації, що становить державну таємницю, засобами інформаційно- комунікаційних технологій, шляхом введення окремої процедури оцінки виконання заходів з кібероборони при здійсненні акредитації з безпеки інформаційно-комунікаційних систем.

6. Додати до принципів, на яких ґрунтується забезпечення кібербезпеки, новий: «проведення на постійній основі періодичного аналізу результативності заходів із забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів силами персоналу цих об'єктів та із залученням уповноважених організацій у цій сфері, включаючи волонтерські організації та їх об'єднання, які акредитовані у встановленому порядку» (або внесені до реєстру виконавців робіт із захисту інформації відповідно до Закону України «Про безпеку інформації та інформаційно-комунікаційних систем».

7. Визначити загальні принципи проведення огляду національної системи кібербезпеки та критичної інформаційної інфраструктури.

8. Встановити вимогу щодо запровадження ризик орієнтованої моделі забезпечення кібербезпеки. При цьому опрацюванню підлягають наступні ризики (рис.3.3).

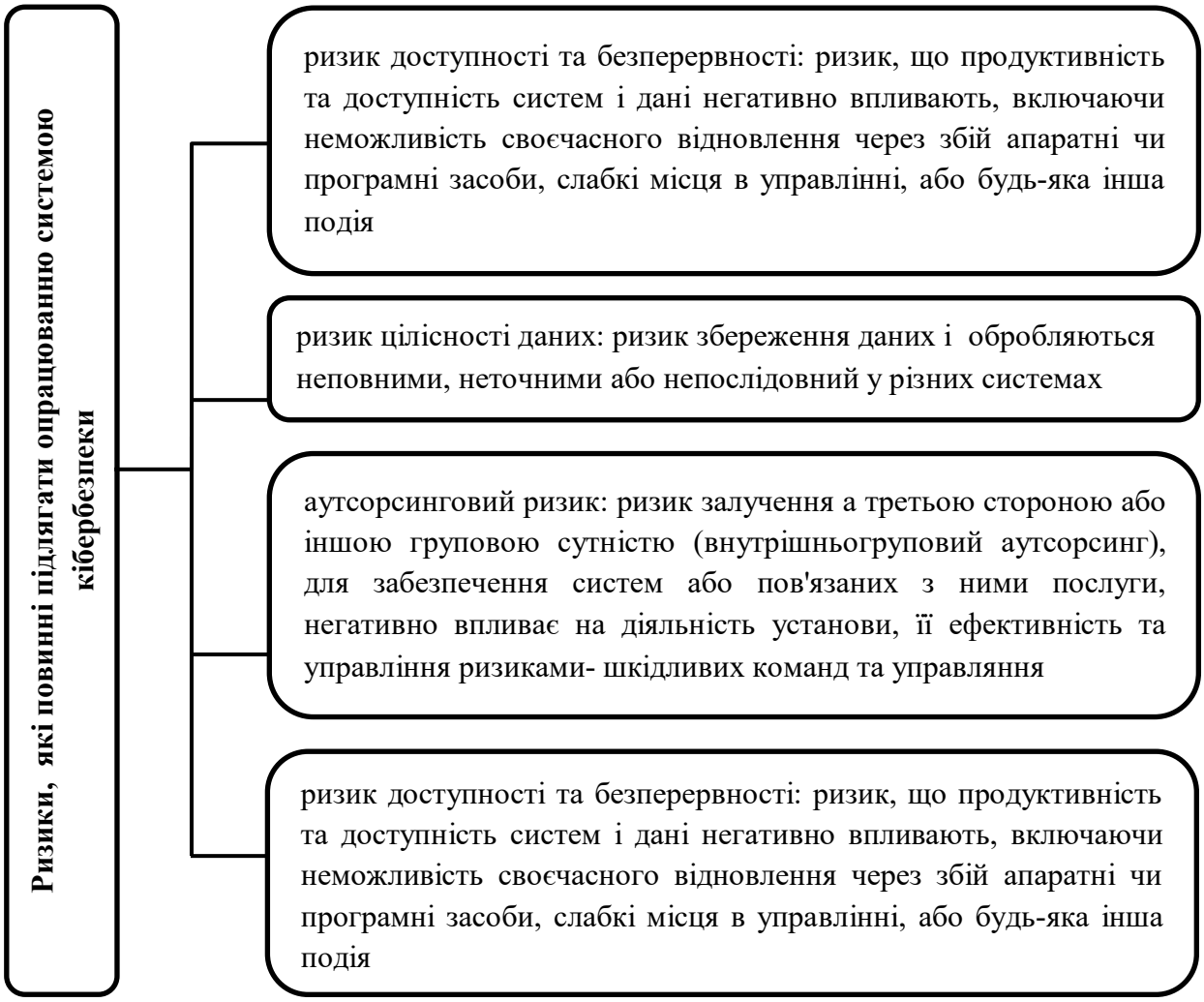


Рис.3.3. Ризики, які повинні підлягати опрацюванню системою кібербезпеки

9. Внести норми щодо порядку визначення цілей та пріоритетів, формування змісту та заходів, термінів їх виконання і способу вимірювання (критерії ефективності – індикатори ключових пунктів), оцінювання ефективності та перегляду Стратегії кібербезпеки України.

10. Фінансування заходів з кібербезпеки – порядок бюджетування та відповідальність за відповідність змісту та розмірів фінансування цілям як Закону так і Стратегії кібербезпеки України.

Національна програма інформатизації, відповідно до Закону України, головною метою має створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [48].

Вибудована у відповідності до цього закону інфраструктура не повною мірою відповідає сучасним умовам і окремі його положення повною мірою ще не реалізовані. У 2020 році були розроблені та внесені до Верховної Ради України пропозиції щодо внесення змін до Закону про НПІ саме з метою забезпечення сумісності державної політики як у сфері інформатизації так і у сфері кібербезпеки та захисту інформації (законопроект № 9166 від 04.10.2020). Основною ідеєю цих пропозицій було долучення Держспецзв'язку до належної участі у реалізації безпекових вимог при формуванні та виконанні завдань (проектів) інформатизації [49].

Так, пропонується, що Держспецзв'язку залучатиметься до: погодження формування та виконання Національної програми інформатизації створення, модернізації інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в тому числі державних реєстрів та баз даних, офіційних веб-сайтів органів державної влади, засобів забезпечення захисту інформації, розробки програмного забезпечення для вказаних систем, розгляду тендерної документації та розробки відповідних пропозицій до неї. При цьому Держспецзв'язку мало б (рис.3.4).

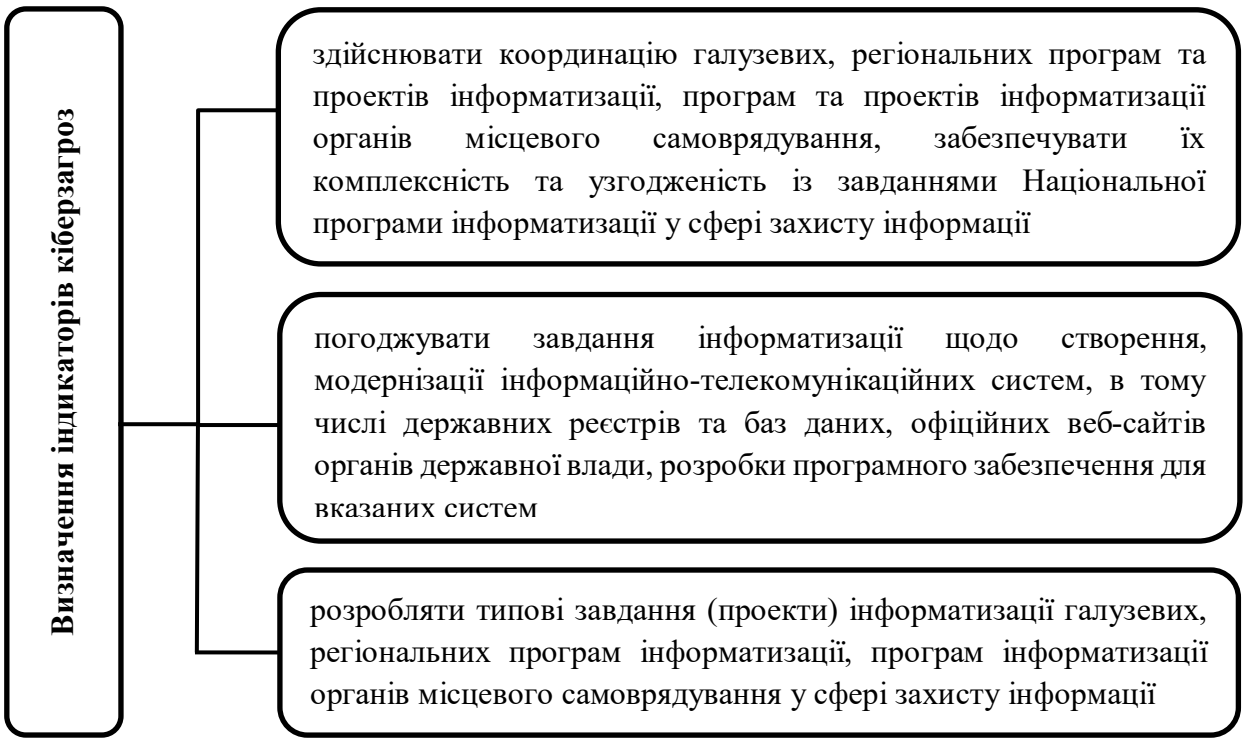


Рис.3.4. Передбачені законодавством завдання Держспецзв'язку [49]

Також передбачалось, щоб замовник Національної програми інформатизації мав [49]:

– погоджувати завдання (проекти) інформатизації щодо створення, модернізації інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в тому числі державних реєстрів та баз даних, офіційних веб-сайтів органів державної влади, засобів забезпечення захисту інформації, розробки програмного забезпечення для вказаних систем, з Держспцентральними органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв’язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України;

– враховувати під час підготовки тендерної документації рекомендації Генерального державного замовника та центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики в сферах організації спеціального зв’язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України в частині технічних, якісних та кількісних характеристик предмета закупівлі в межах їх компетенції;

Іншою важливою ініціативою щодо удосконалення законодавства у сфері інформатизації слід розглядати інший документ – Перелік обов’язкових етапів робіт та/або надання послуг під час створення (модернізації), адміністрування та забезпечення функціонування засобів інформатизації. В Законі про НПІ засоби інформатизації – це електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій. Таким чином, засоби інформатизації мають бути забезпечені відповідними запевненнями (гарантіями), що їх застосування не впливатиме негативно на рівень кібербезпеки, зокрема, та рівеь захищеності (безпеки) інформації при їх використанні, взагалі [50].

Отже, засоби інформатизації мають відповідати вимогам з безпеки. Визначити перелік вимог з безпеки до засобів інформатизації, враховуючи їх широкоохоплююче законодавче визначення досить важко, доцільно такі вимоги встановлювати з урахуванням потенційного способу та місця їх застосування. При цьому головним суб'єктом, хто встановлюватиме такі вимоги буде замовник засобів інформатизації. Таким чином, ґрунтуючись на вимогах законодавства у сфері захисту
інформації, можливо сформувати набір кроків, виконання яких під час розробки засобів інформатизації надасть можливість забезпечити відповідність як таких засобів так і систем, де передбачається їх застосування, цим вимогам. Тому пропонується наступна послідовність обов'язкових етапів робіт щодо засобів інформатизації:

1. Розроблення техніко-економічного обґрунтування на створення, адміністрування, забезпечення функціонування або модернізації засобів інформатизації та захисту інформації, створення або модернізацію комплексної системи захисту інформації ІТС, в якій передбачається їх застосування, або системи управління безпекою інформації замовника.

2. Розроблення технічного завдання на створення або модернізацію засобів інформатизації, їх адміністрування та забезпечення функціонування, захисту інформації, створення або модернізацію комплексної системи захисту інформації ІТС, якій передбачається їх застосування, або системи управління безпекою інформації замовника. Проведення експертних досліджень засобів інформатизації на відсутність недокументованих функцій та, за необхідності, вимогам законодавства у сфері захисту інформації засобів інформатизації (їх складових частин), які використовуються для реалізації послуг безпеки і не мають підтвердження відповідності.

3. Проведення навчання фахівців для забезпечення адміністрування та забезпечення функціонування засобів інформатизації, а також підрозділів захисту (безпеки) інформації, складання заліків за результатами навчання.

Проведення випробувань створених або модернізованих засобів інформатизації.

4. Проведення робіт із створення та оцінки відповідності комплексних систем захисту інформації ІТС, в яких передбачається застосування засобів інформатизації, які створюються або модернізуються, або змін до КСЗІ, якщо використання таких засобів має вплив на рівень безпеки інформації в ІТС і воно не передбачалося раніше.

5. Розроблення (удосконалення) організаційно-розпорядчих документів для забезпечення експлуатації засобів інформатизації та безпеки інформації при їх використанні: положення, порядок обробки інформації, регламент роботи, політика управління ризиками для безпеки інформації.

6. Отримання підтвердження відповідності комплексної системи захисту інформації або системи управління інформаційною безпекою інформації при створенні або модернізації засобу інформатизації.

7. Введення засобів інформатизації та комплексної системи захисту інформації (її складової частин) в промислову експлуатацію.

Отже, органам державної влади рекомендовано розширити варіанти огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, а саме не тільки як автономну процедуру та складову комплексного огляду сектору безпеки та оборони, а також передбачити його проведення у складі процедури періодичного проведення огляду національної системи кібербезпеки. Крім цього слід внести відповідні зміни до Закону ОЗКБ, Закону України «Про національну безпеку України» щодо автономного застосування періодичного проведення огляду національної системи кібербезпеки або у складі комплексного огляду сектору безпеки та оборони. Також існує необхідність розробки вичерпних вимог до змісту заходів з оцінювання захищеності інформації від кіберзагроз, порядку виконання цих заходів, вимог до персоналу та вимог до оцінювання ефективності такого оцінювання.

3.3. Вплив державно – приватного партнерства на розвиток механізмів захищеності інформації та інформаційно-телекомунікаційних систем

В рамках дослідження існуючих механізмів публічного управління досліджено різні організаційно-технічні механізми визначення стану захищеності інформації та систем, що її обробляють: оцінювання стану захищеності державних інформаційних ресурсів, державний контроль за станом технічного та криптографічного захисту інформації, оцінювання захищеності інформації, що не становить державної таємниці, та проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури. При оцінюванні стану захищеності державних інформаційних ресурсів здійснюється детальний аналіз мереж і систем з точки зору потенційного зловмисника. Суть тесту полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту інформаційної системи. В ході тестування роль зловмисника відіграє спеціаліст, який повинен визначити рівень захищеності, виявити вразливості, ідентифікувати найбільш вірогідні шляхи злому і визначити наскільки добре працюють засоби виявлення і захисту інформаційної системи від атак на підприємстві [51, С. 134].

Завдання оцінки – виявлення вразливостей інформаційної системи; використання виявлених вразливостей для отримання несанкціонованого доступу чи здійснення несанкціонованого впливу на інформацію для демонстрації наявності вразливостей і існування високоймовірної загрози інформаційної системи; оцінка поточного стану системи захисту інформації інформаційної системи; вироблення рекомендацій щодо підвищення ефективності захисту інформації в інформаційній системі

Державний контроль за станом технічного та криптографічного захисту інформації передбачає проведення в рамках інспектування аналізу та виявлення порушень вимог законодавства у сфері захисту інформації. За результатами проведення контролю складається акт з виявленими

порушеннями та вимогами щодо їх усунення. Не усунення порушень, викладених в акті, має результатом заборону оброблення в системі інформації, вимога щодо захисту якої встановлена законом.

Реалізація перших двох механізмів здійснюється Держспецзв'язку. Третій механізм – оцінювання захищеності інформації, що не становить державної таємниці. Цей механізм регулюється шляхом ліцензування господарської діяльності у галузі технічного захисту інформації, може застосовуватись шляхом залучення підприємства ліцензіата в галузі технічного захисту інформації. Відповідно до Переліку видів господарської діяльності, які підлягають ліцензуванню, цей механізм передбачає атестацію комплексів технічного захисту інформації та експертні оцінювання у сфері технічного захисту інформації. Ліцензійними умовами провадження цього виду діяльності передбачена, зокрема, наявність нормативних документів технічного захисту інформації. Основним з них є «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Згідно з цим документом критерієм захищеності інформації є відповідність архітектури та параметрів програмно-апаратних засобів об'єкта оцінювання чіткому регламенту – комплексній системі захисту інформації (КСЗІ – далі). За результатами такого способу оцінювання видається експертний висновок (є власником замовника експертизи та, зазвичай, не публікується). Експертний висновок є підставою для видачі атестата відповідності КСЗІ. Наявність такого атестата є умовою оброблення інформації з обмеженим доступом або інформації, вимога щодо захисту якої встановлена законом, згідно з Законом України «Про захист інформації в ІТС».

Четвертий механізм – незалежний аудит інформаційної безпеки на об'єктах критичної інфраструктури. Забезпечує функціонування системи такого аудиту, а також визначення вимог і порядку його проведення здійснює Кабінет Міністрів України, забезпечують його проведення суб'єкти забезпечення кібербезпеки, а організація його проведення покладається на власників/розпорядників об'єктів критичної інфраструктури [51, С. 135].

За результатами аналізу цих механізмів запропоновано: на даному етапі розширити коло суб’єктів, що на законодавчих підставах, не вступаючи в конфлікт з положеннями статті 361 КК України (незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж), за згодою власника системи та, за необхідності, за погодженням з уповноваженими органами будуть здійснювати оцінювання захищеності державних інформаційних ресурсів і за результатами яких будуть видаватися відповідні рекомендації. При цьому вимоги до суб’єктів проведення оцінювання за ліцензованим видом діяльності, його цільова функція та зміст перевірок мають постійно відповідати рівню можливих загроз в кіберпросторі.

В подальшому необхідно забезпечити поступове злиття обох видів оцінювань та їх трансформація і об’єднання в незалежний аудит інформаційної безпеки за міжнародними стандартами та передовими практиками. У такому мотиваційному механізмі, як один із першочергових кроків розбудови державно-приватної взаємодії у сфері кібербезпеки, є удосконалення ліцензування господарської діяльності у сфері захисту інформації шляхом унесення змін до ліцензійних умов щодо надання послуги у галузі технічного захисту інформації з оцінювання захищеності інформації, що не становить державної таємниці (Додаток Е).

Державно-приватне партнерство (ДПП – далі) у сфері кібербезпеки, визначає напрямки розвитку кібербезпеки та причини для взаємодії уряду і бізнес-структур наступним чином [52, С. 200]:

1. Економічні інтереси для участі приватного сектору, які можуть, наприклад, мати такі цілі:

1. 1 створення органу, який допоможе визначити бар'єри для розвитку галузі кібербезпеки та створити умови для експорту продуктів кібербезпеки;

1. 2 співпраця з державним сектором, наприклад, з фінансовим сектором у сфері боротьби з кіберзлочинністю;

1. 3 можливість впливати на процес захисту свого бізнесу від зайвих або надмірно обтяжливих перестроїв.

2. Нормативні вимоги:

2.1 імплементація конкретного закону, коли це вимагається, і державна адміністрація вирішить, що рамки ДПП будуть найкращим способом цього зробити вбо спеціального закону щодо ДПП, який забезпечує чітку основу для приватно-державного співробітництва та співпраці;

2.2 підвищення якості зв'язків з громадськістю. У цьому випадку уряд дозволяє приватному сектору надати внесок у нове законодавство, а також спільно працювати над розробкою національної стратегії кібербезпеки;

2.3 соціальні інтереси – широке обговорюваня проблем кібербезпеки в державі та встановлювати кібербезпеку на високому рівні в політичному порядку денному.

Напрямки можливого ДПП визначаються такі: оброблення інцидентів та управління кризами; дослідження та аналіз; розробка передової практики та рекомендацій; обмін інформацією; ранні попередження; внавчання; підвищення рівня обізнаності; технічна оцінка; визначення стандартів; довідкова служба; управління кризовими ситуаціями; планування стійкості; планування надзвичайних ситуацій; аудит безпеки; стратегічне планування; аналіз ризиків. У зв’язку з цим можна надати такі рекомендації щодо поліпшення державно-приватного партнерства [51, С. 200]:

– мотивація приватного сектору для участі повинна бути пріоритетним завданням при формуванні ДПП, для успішної та ефективної якого необхідні ресурси;

– учасники повинні погодитися з правовими основами при створенні ДПП. Поки немає юридичної бази для співпраці, весь процес створення та розвитку ДПП буде повільним і неефективним. Правовою основою може бути національний правовий акт або Меморандум про взаєморозуміння, оскільки кібербезпека - це міжгоризонтальна сфера, в якій, як правило, багато державних структур залучаються разом з різними приватними компаніями;

– державні установи повинні керувати ДПП або національним планом дій щодо ДПП для усунення розбіжностей між ключовими державними установами: Міністерство внутрішніх справ, Міністерство оборони, Міністерство економіки та розвитку. Державні установи, які беруть участь у ДПП, повинні знати заздалегідь чого вони хочуть досягти, що сприятиме їхньому внеску та що приватний сектор повинен сприяти;

– ДПП повинні інвестувати у внутрішнє приватне та приватне співробітництво та державно-державне співробітництво ДПП - це співпраця приватно-приватного, публічно-державного та приватно-публічного. Правильний рівень діалогу та взаєморозуміння між державними установами часто є запорукою успішного ДПП. Те саме стосується приватного сектору. Успішне ДПП інтегрує не лише приватну адміністрацію та галузь, але й різні суб'єкти господарювання (наприклад, енергетичні компанії, банки, телекомунікації);

– учасники ДПП повинні інвестувати у відкриту комунікацію та прагматичний підхід до побудови ДПП;

– представникам уряду слід дозволити брати участь у засіданнях за угодою про нерозголошення;

– малі та середні підприємства також повинні брати участь у ДПП.

Таким чином, можна зробити висновок, що державно-приватне партанетство щодо кібербезпеки може бути в напрямках самого широкого спектра: від взаємодії в нормативному регулюванні до навчання і спільного планування заходів із забезпечення стійкості щодо кіберінцидентів. Стратегія кібербезпеки України одним із принципів забезпечення кібербезпеки України визначає державно-приватне партнерство, широку співпрацю з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту.

Розглядаючи можливість застосування українського законодавства у цій сфері, а саме Закону України «Про державно-приватне партнерство», слід зазначити. Що ним окреслена лише одна сфера – управління об’єктами

державної власності за напрямками (стаття 4): виробництво, транспортування і постачання тепла та розподіл і постачання природного газу; будівництво та/або експлуатація автострад, доріг, залізниць, злітно- посадкових смуг на аеродромах, мостів, шляхових естакад, тунелів і метрополітенів, морських і річкових портів та їх інфраструктури; машинобудування; збір, очищення та розподілення води; охорона здоров'я; туризм, відпочинок, рекреація, культура та спорт; забезпечення функціонування зрошувальних і осушувальних систем; поводження з відходами, крім збирання та перевезення; виробництво, розподілення та постачання електричної енергії; надання соціальних послуг, управління соціальною установою, закладом; виробництво та впровадження енергозберігаючих технологій, будівництво та капітальний ремонт житлових будинків, повністю чи частково зруйнованих внаслідок бойових дій на території проведення антитерористичної операції; встановлення модульних будинків та будівництво тимчасового житла для внутрішньо переміщених осіб; надання освітніх послуг та послуг у сфері охорони здоров'я; управління пам'ятками архітектури та культурної спадщини.

Крім цього, Законом ОЗКБ також визначено, що одним із шляхів функціонування національної системи кібербезпеки та принципів державно-приватної взаємодії є обмін інформацією про інциденти кібербезпеки між суб’єктами забезпечення кібербезпеки у порядку, визначеному законодавством. Суб’єкти забезпечення кібербезпеки в межах своєї компетенції здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз. Держспецзв’язку, як один з основних суб’єктів національної системи кібербезпеки, інформує про кіберзагрози та відповідні методи захисту від них, а також координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту [15]. Порівнюючи норми українського законодавства щодо інформування про кіберінциденти з вимогами законодавств інших країн та ЄС, наведеними в підрозділах 1.2 та 1.3, можливо зазначити, що Україні необхідно прикласти належні зусилля в дослідження, обґрунтований вибір та імплементацію в своє правове поле

відповідних норм і вимог. Основними принципами, які мають бути покладені в Закон ОЗКБ, щодо інформування про кіберінцидент, є (рис.3.6).

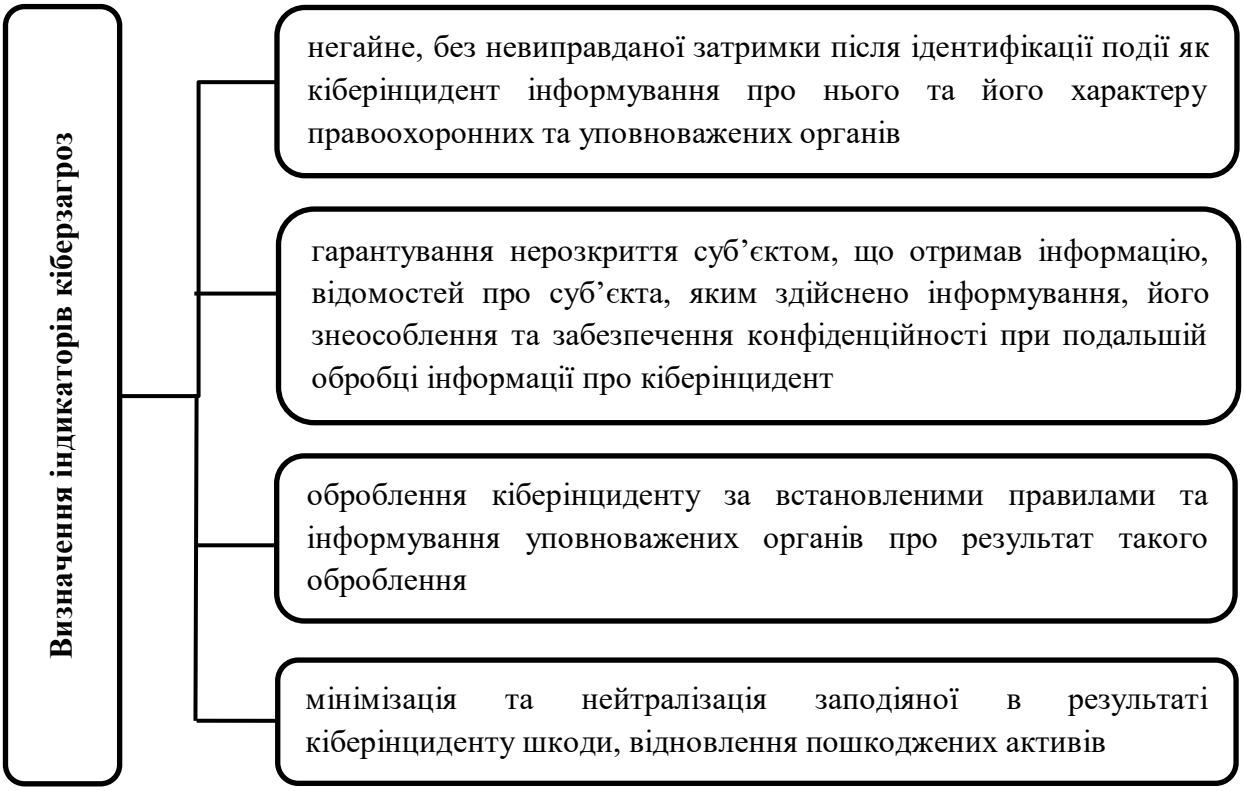


Рис. 3.6. Основнимі принципи, які мають бути покладені в Закон ОЗКБ, щодо інформування про кіберінцидент

Слід відмітити, що такий спосіб нормативного врегулювання оброблення кіберінциденту запровадить базис для подальшого підвищення стійкості об'єктів кібератак та сприятиме підвищення рівня зрілості суб'єкта, щодо якого здійснюється кібератака.

Таким чином, реалізація державно-приватної взаємодія має бути законодавчо встановлена за такими напрямками: спільність цілей та гарантування реалізації взаємних інтересів держави та бізнес-структур, прозорості у відносинах при реалізації взаємодії, визначення можливих форм нормативного закріплення реалізації взаємодії тощо. Такі зміни доцільно вносити саме у Закон України «Про основні асади забезпечення кібербезпеки України» на підставі необхідності доповнення нормами саме щодо забезпечення розвитку та реалізації норм статті 10.

ВИСНОВКИ

Магістерська робота присвячена дослідженню теротичних основ та наданні практичних рекомендацій з вдосконалення механізмів публічного управління у сфері кібербезпеки в сучасних умовах. Результати, одержані в процесі проведення дослідження, дозволяють зробити такі висновки:

1. На снові аналізу трактувань різними авторами сутності поняття «кібербезпека» визначено, що захист важливих цифрових систем та баз даних від несанкціонованого доступу є важливою передумовою для розвитку сучасного суспільства, а своєчасне виявлення, запобігання та нейтралізація реальних або потенційних загроз національній безпеки України в кіберпросторі сприяє вдосконаленню політики забезпечення безпеки в цифровому просторі країни. Зауважено, окільки урядові, військові, фінансові та медичні організації збирають, обробляють та зберігають велику кількість стратегічно важливих даних, питання їх захисту є приоритетом системи публічного управління в галузі кібербезпеки, для захисту якої розроблена низка законодавчих актів та імплементовані міжнародні стандарти.

2. Досліджено основні нормативно – правові акти, що визначають розвиток національної системи кібербезпеки дали змогу сформувати ієрархічну інфраструктуру законодавства у сфері кібербезпеки з метою впорядкування та систематизації, в також викремити напрямки, в яких здійснюється законодавча діяльність,зокрема: формування та забезпечення функціонування Державного реєстру об’єктів критичної інформаційної інфраструктури; розробка нормативно – правових актів, які регламентують діяльність основних суб’єктів кібербезпеки України, їх конкретні завданн, а також формують систему органів що здійснює їх координацію; процедури збору інформації про стан об’єктів інформаційної критичної інфраструктури та оперативного реагування системою кібербезпеки на кіберінценденти та кібератаки. Однак забезпечення взаємодії між групами реагування на комп’ютерні надзвичайні ситуації, а також їх взаємодії з глобальними

центрами кіберзахисту, залишається викликом. Запропоновано наступний механізм взаємодії: координація оперативної діяльності груп реагування, облік та публікація на публічних ресурсах усієї контактної інформації для зв’язку з ними та інформування уповноважених осіб. Підкреслено, оскільки актуальною залишається проблема розробки та впровадження організаційно-правових механізмів управління розвитком кіберзахисту критичної інформаційної інфраструктури України, доцільним є врахуванням міжнародного досвіду в цій сфері, насамперед країн Європейського Союзу.

3. Розглянуто та узагальненено міжнародний досвід щодо формування та реалізації механізмів забезпечення публічної політики інформаційної безпеки, що дало змогу визначити пріоритетні напрямки розвитку відповідних національних механізмів в Україні, а саме: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів в національних інтересах; створення загальної системи охорони даних; сприяння міжнародній взаємодії у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури.

4. Визначено, що у разі виявлення кіберінцидентів та кібератак, що можуть становити загрозу національній безпеці або обороноздатності держави, Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України у встановленому порядку інформує Національний координаційний центр кібербезпеки, а також надає необхідну інформацію з Державного реєстру об’єктів критичної інфраструктури, для формування Стратегії кібербезпеки України та інших стратегічних рішень в цій сфері.

5. З’ясовано, що лише 1 місяць 2023 року сталося 2,7 більше хакерських атак різного виду, ніж за аналогічний період 2021 року. Система виявлення вразливостей і реагування на кіберінциденти та кібератаки виявила 11,5 мільйонів підозрілих подій інформаційної безпеки протягом ІІІ кварталу 2023 року. Крім того, було оброблено 12 000 критичних подій інформаційної

безпеки, які включали ймовірність кіберінцидентів, виявлених через вторинні аналіз і фільтрація підозрілих подій ІБ. Аналітики безпеки одночасно задокументували та обробили 355 кіберінцидентів. Кількість зареєстрованих кіберінцидентів зросла на 46% порівняно з ІІІ кварталом 2023 року. Для виявлення вразливостей та реагування на кіберінциденти та кібератаки державні, енергетичні та військові сектори підключили до 14 нових систем кіберзахисту. Також у ІІІ кварталі 2023 року проросійські хакерські групи зафіксували 202 кібератаки, що на 26% менше, ніж у попередньому кварталі.

6. Звуважено, що оскільки в Україні на законодавчому рівні визначено необхідність та пріоритетність здійснення міжнародного співробітництва в кібербезпековій сфері з використанням організаційно-правових та фінансових механізмів міжнародного співробітництва у сфері кібербезпеки з Україною, проведено порівняння з існуючими спроможностями України в цій сфері, яке вона здійснює як на двосторонній основі з окремими державами, так і з їх об'єднаннями. Аналіз практичної релізації заходів коорепації в галузі захисту цифрового середовища показав, що незважаючи цілу низку розроблених та імплементованих організаційноправових механізмів державного управління міжнародним співробітництвом, однією з головних проблем залишається проблема координованості дій суб'єктів кібербезпеки, і яка є основною причиною недостатньої ефективності державної політики в цій сфері. Виокремлено напрямки удосконалення національних механізмів державного управління на основі практики міжнародного співробітництва, які доцільно буде додати в оновлену редакцію Стратегії кібербезпеки України з метою позбавлення вад її чинної версії та містити більш конкретні завдання і заходи із забезпечення кібербезпеки з можливістю їх коригування відповідно до загроз у кіберпросторі.

7. Узагальнено напрямки вдосконалення публічного управління задля підвищення ефективності забезпечення кібербезпеки України, серед яких можна виділити: впровадження механізмів встановлення відповідності змісту щорічних заходів з реалізації Стратегії кібербезпеки України її цілям,

осучаснення принципів планування та контролю за виконанням цих заходів; розширення кола суб'єктів-учасників виконання щорічних планів заходів з реалізації заходів кібербезпеки України. Необхідно також доповнити положення щодо запровадження сучасних механізмів стратегічного планування завданнями з формування переліку та планів забезпечення стійкості об'єктів критичної інформаційної інфраструктури, впровадження системного та інтегрованого підходу до управління ризиками кібербезпеці на національному рівні, що сприятиме підвищенню її результативності.

8. Рекомендовано органам державної влади розширити варіанти процедур огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, а саме не тільки як автономну процедуру та складову комплексного огляду сектору безпеки та оборони, а також передбачити його проведення у складі процедури періодичного проведення огляду національної системи кібербезпеки. Крім цього слід внести відповідні зміни до Закону ОЗКБ, Закону України «Про національну безпеку України» щодо автономного застосування періодичного проведення огляду національної системи кібербезпеки або у складі комплексного огляду сектору безпеки та оборони. Також існує необхідність розробки вичерпних вимог до змісту заходів з оцінювання захищеності інформації від кіберзагроз, порядку виконання цих заходів, вимог до персоналу та вимог до оцінювання ефективності такого оцінювання.

9. Зазначено, що реалізація державно-приватної взаємодія має бути законодавчо встановлена за такими напрямками: спільність цілей та гарантування реалізації взаємних інтересів держави та бізнес-структур, прозорості у відносинах при реалізації взаємодії, визначення можливих форм нормативного закріплення реалізації взаємодії тощо. Такі зміни доцільно вносити саме у Закон України «Про основні асади забезпечення кібербезпеки України» на підставі необхідності доповнення нормами саме щодо забезпечення розвитку та реалізації норм статті 10.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. № 9. С. 100 – 108.

2. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія: «Юридичні науки»*. 2019. № 2. С. 23 – 28.

3. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: «Державне управління»*. 2019. № 1. С. 140 – 145.

4. Горун О. Ю. Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. *Інформація і право*. 2021. № 2 (37). С. 93 – 102.

5. Яковлєв П. О. Об'єкт і предмет державного регулювання у сфері забезпечення інформаційної безпеки України. *Право і суспільство*. 2020. № 3. С.178 – 183.

6. Сливка М.М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний факультет Запорізького національного університету*. 2022. № 10. С. 489 – 491.

7. Станіславський Т. Розвиток міжнародного співробітництва України у сфері кібербезпеки. *Актуальні проблеми державного управління*. 2019. № 3. С. 58 – 67. URL:

8. Дешко Л.М., Бонарєва К.Д. Кібербезпека в Україні: Національна стратегія та міжнародне співробітництво. *Порівняльно-аналітичне право*. 2018. № 2. С. 136 – 158.

9. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України: дисертація ... канд. юрид. наук, спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / В.В. Бухарєв; наук. кер. А.М. Куліш. Суми: Ун-т сучасних знань, 2018. 221 с.

10. Лахно В. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту. *Безпека інформації*. 2022. Т. 22. № 1. С. 44 – 50.

11. Євсюкова О. В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. Державне управління: удосконалення та розвиток. 2021. № 2. URL: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf. (дата звернення 28.12.2023).

12. Шинкаренко А.Ю., Ставицький О.В., Кібербезпека як один з механізмів забезпечення стабільного розвитку економікив Україні. Електронний архів НТУУ «КПІ» ім.. І. Сікорського. URL: https://ela.kpi.ua/bitstream/123456789/22611/1/2017-11_5-09.pdf. (дата звернення 28.12.2023).

13. Петров С.Г. Стан наукової розробки проблеми захисту державних електронних інформаційних ресурсів в Україні. Науковий вісник Ужгородського національного університету. *Серія ПРАВО*. 2020. № 61. Т. 2. С. 20 – 23.

14. Петров С. Г. Захист державних електронних інформаційних ресурсів України. *Інформація і право*. 2020. № 3 (34). С. 62 – 68. URL: https://ippi. org.ua/sites/default/files/9_17.pdf. (дата звернення 28.12.2023).

15. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення 28.12.2023).

16. Конституція України 1996 р. Відомості Верховної Ради України. 1996. № 30. С. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-% D0%B2%D1%80. (дата звернення 28.12.2023).

17. Про національну безпеку України: Закон України від 21.06.2018 року № 2469-VIII. Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/ show/2469-19#Text. (дата звернення 28.12.2023).

18. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017. (дата звернення 28.12.2023).

19. Про кіберзлочинність: Конвенція РЄ від 23 листопада 2001 року. Офіційний вісник України. 2007. № 65. Ст. 253. URL: https://zakon.rada. gov.ua/laws/show/994_575#Text. (дата звернення 28.12.2023).

20. Про електронні комунікації: проект Закону України від 16.12.2020 № 1089-IX. Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/1089- 20#Text. (дата звернення 28.12.2023).

21. Про критичну інфраструктуру та її захист: проект Закону України від 17.03.2021 р. № 5219-1. Єдиний веб - портал органів виконавчої влади в України. URL: https://www.kmu.gov.ua/bills/proekt-zakonu-pro-kritichnu-infrastrukturu-ta-ii-zakhist . (дата звернення 28.12.2023).

22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України 2021 – 2025»: Указ Президента України від 26.06.2021 р. № 447/2021. Офіс Президента України. URL: https://www.president.gov.ua/documents/4472021-40013. (дата звернення 28.12.2023).

23. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. Офіційний вісник України. 2016. № 69. Ст. 2332. URL: https://zakon.rada.gov.ua/laws/show/563-2016-п#Text. (дата звернення 28.12.2023).

24. Заскока Ю. Державна політика та правові механізми забезпечення кібербезпеки україни: ретроспектива та сучасністЬ. *Наукові інновації та передові технології*. 2022. № 10 (12). URL: http://perspectives.pp.ua/index.php/nauka/article/download/2591/2597

25. Milov O., Milevskyi S., Korol O. Developing an advanced classifier of threat for security agent behavior models. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 4 (37). 105 – 112.

26. An official website of the European Union. URL: https://europa.eu/european-union/. (дата звернення 28.12.2023).

27. European cebercrime centre. An official website of the European Union

Agency for Law Enforcement Cooperation. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. (дата звернення 28.12.2023).

28. Kaponig H. Austria's National Cyber Security and Defense Policy. Connections. 2020. 19 (1). 21 – 37.

29. Tvaronavičienė M., Plėta T., Della Casa S., & Latvys, J. Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*. 2020. 2 (4). 802 – 813.

30. Brzostek A. Germany's Cybersecurity Policy. *Teka Komisji Prawniczej PAN Oddział w Lublinie*. 2022. 15 (2). 61 – 72.

31. Del-Real C., Díaz-Fernández A. M. Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *International Cybersecurity Law Review*. 2022. 3 (2). 313 – 343.

32. Angelini M., Ciccotelli C., Franchina L., Marchetti-Spaccamela A., Querzoni L. Italian National Framework for Cybersecurity and Data Protection. In Privacy Technologies and Policy. *Springer: Cham. Switzerland*. 2020. 127 – 142.

33. Jacuch A. Comparative Analysis of Cybersecurity Strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies. *Online Journal Modelling the New Europe*. 2021. 37. 102 – 120.

34. 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): Регламент Європейського Парламенту І Ради (ЄС) 2016/679 від 27 квітня 2016 року. Офіційний вісник Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text. (дата звернення 28.12.2023).

35. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: постанова Кабінету Міністрів України від 23.12.2020 р. № 1295. URL: https:// zakon. rada. gov.ua/laws/show/1295-2020-%D0%BF#Text. (дата звернення 28.12.2023).

36. Деякі питання функціонування Національної телекомунікаційної мережі: постанова Кабінету Міністрів України від 16.12.2020 р. № 135. URL: https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text. (дата звернення 28.12.2023).

37. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475 – IV. Відомості Верховної Ради. 2006, № 30, Ст.258. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text . (дата звернення 28.12.2023).

38. Про затвердження Положення про державний контроль за станом технічного захисту інформації: наказ Адміністрації Держспецзв'язку України від 16.05.07 р. № 87. Офіційний вісник України. 2007. № 50. Ст. 2037. URL: https://zakon.rada.gov.ua/laws/show/z0785-07. (дата звернення 28.12.2023).

39. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: постанова Правління Національного банку України від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text. (дата звернення 28.12.2023).

40. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023. URL: https://scpc.gov.ua/api/files/22c75b41-d1d8-4da6-bd46-fa5489af9c6e. (дата звернення 28.12.2023).

41. Потій О., et al. Публічне управління інституціональним розвитком у сфері кіберзахисту. Науковий вісник: Державне управління. 2021. № 3 (9). 136 – 162. URL: https://nvdu.undicz.org.ua/index.php/nvdu/article/view/193/186

42. Гуцалюк М.В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. *Інформація і право*. 2021. № 4 (39). С. 141 – 147.

43. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 . (дата звернення 28.12.2023).

44. План дій Україна – ЄС у сфері «Юстиція. Свобода. Безпека» URL: https://minjust.gov.ua/m/plan-diyukraina-es-u-sferi-yustitsii-svobodi-ta-bezpeki-12

24. (дата звернення 28.12.2023).

45. Звіт про виконання Угоди про асоціацію між Україною та Європейським Союзом за 2022 рік. URL: https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/zvit_pro_vyko nannya _ugody_pro_asociaciyu_za_2022_rik.pdf. (дата звернення 28.12.2023).

46. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *International relations, part «Political science»*. 2022. № 18 – 19 (2). URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389. (дата звернення 28.12.2023).

47. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. А. В. Жилін, О. М. Шаповал, О. А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

48. Про національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. Відомості Верховної Ради України. 1998. № 27-28, ст.181. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80. (дата звернення 28.12.2023).

49. Про внесення змін до Закону України «Про Національну програму інформатизації»: законопроект Державного управління справами від 04.10.2018 № 9166. URL: https://ips.ligazakon.net/document/XH72M00Q. (дата звернення 28.12.2023).

50. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації: постанова Кабінету Міністерства України від 04.02.1998 № 121. URL: https://zakon.rada.gov.ua/laws/show/121-98-%D0%BF#Text. (дата звернення 28.12.2023).

51. Дорогих С. О. Щодо питань інформаційної безпеки як напряму інформаційної політики України в умовах війни. Інформація і право. 2022. № 2 (41). С. 133 – 137.

52. Малахов Г.Б. Шляхи удосконалення державно-приватного партнерства у сфері кібербезпеки України. *Інформація і право*. 2023. № 4 (47). С. 197 – 206.

53. Про державно-приватне партнерство: Закон України від 01.07. 2010 р. № 2404-VI. Відомості Верховної Ради України. 2010, № 40, Ст.524. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text. (дата звернення 28.12.2023).

ДОДАТКИ

Додаток А

Бондаренко В. О.
студент 2 курсу магістратури
Університету митної справи та фінансів, Дніпро
(науковий керівник – Ковальов В.Г., к.держ.упр., доц.,
кафедри публічного управління та митного адміністрування
Університету митної справи та фінансів, Дніпро)

МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Сьогодення вимагає від кожної країни відповідності своїх спроможностей у захисті конституційних прав та свобод своїх громадян, особливо у тих сферах суспільних відносин, де застосовність продукції інформаційно-комунікаційних технологій (ІКТ - далі) має визначальний вплив на життєво важливі послуги, ведення бізнесу, безпеку всіх видів комунікацій, життєдіяльності громадян, суспільства та держави. Крім того, проникнення таких технологій у повсякденне життя вимагає нових знань в новому середовищі – кіберпросторі, від якого слід очікувати не тільки великої кількості сервісів та благ, а й розвитку існуючих та створення нових загроз. Ці загрози пов'язані із застосуванням механізмів несанкціонованого втручання в роботу систем та порушення безпеки інформації, яку вони обробляють, постійний розвиток індустрії розроблення та широке використання різного роду шкідливого та уразливостей широковживаного програмного забезпечення. Пильна увага громадськості до питань впровадження ІКТ в широкий спектр суспільних відносин, щоденно зростаюча небезпека від їх використання робить актуальним завдання системного аналізу національної системи кібербезпеки, її вад, обґрунтування напрямів її модернізації.

Ст. 7 Конституції України зазначає, забезпечення інформаційної безпеки України є однією із найважливіших функцій держави та справою всього Українського народу [1]. Відповідно до ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», система державного управління кібербезпекою є досить розгалуженою і поєднує у собі значну кількість органів владі, зокрема: Раду національної безпеки і оборони України, Міністерство внутрішніх справ України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, розвідувальні органи та інші [2]. З огляду на вищевикладене, держава бере на себе обов'язок здійснювати захист громадян від негативного впливу та делегує повноваження по протидії даному явищу компетентним органам.

В той же час, в національній системі кібербезпеки існує низка прогалин, які негативним чином впливають на її ефективність, серед яких можна виділити: майже повний імпорт продукції ІКТ, низька координованість виконання загальнодержавних проектів інформатизації, неефективне

бюджетування забезпечення кібербезпеки, низька культура кібербезпеки в усіх сферах суспільного та особистого життя.

Важливе значення в забезпечення кібезбезнеки системи державного управління покладається на запобігання та протидію хакерським атакам, що значно активізувалися у воєнний період. У порівнянні з 2021 за період 2022 – 2023 рр. відбувається втричі більще подібних атак (199 проти 77) щомісяця. Цілі подібних атак наведені в табл.1 [3].

Таблиця 1

Хакерські атаки на кіберпростір України

Сектори проти яких були спрямовані хакерські актаки		
Комерційний сектор	Телеком та програмне забезпечення	Засоби масової інформації
35 %	20 %	17 %
Уряд та місцеві органи влади	Фінансовий сектор	Медіа
15 %	5 %	3 %
Сектор безпеки та оборони	Енергетика	Інші
3 %	2 %	1 %

Слід також зауважити, що загальна спроможність суб'єктів кібербезпеки протидіяти кіберзагрозам в державному секторі знаходиться на низькому рівні (на рівні 36 %), для приватного сектора цей показник складає 62 %. Із зазначеного випливають наступні для системи днржавного управління: потреба у покращнні кадрового потенціалу; створення стійкої системи національної системи кібербезпеки та підвищення ролі кібербезпеки у всіх державних процесах [3]. Отже, найбільш перспективними напрямами розвитку механізмів державного управління кібербезпеки в сучасних умова є: посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі, розвиток потенціалу забезпечення кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації, модернізація національної системи кібербезпеки України.

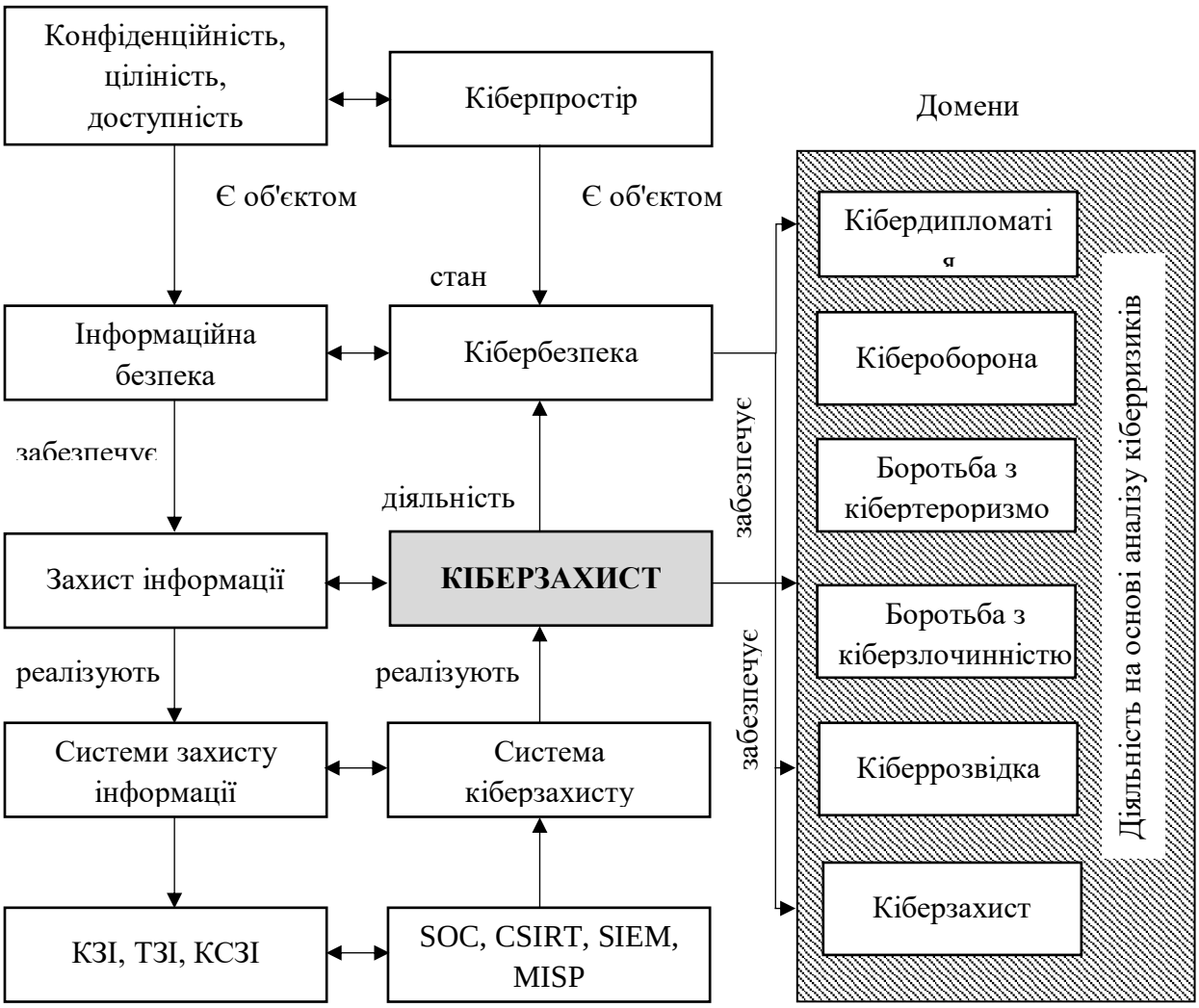
Список використаних джерел:

1. Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

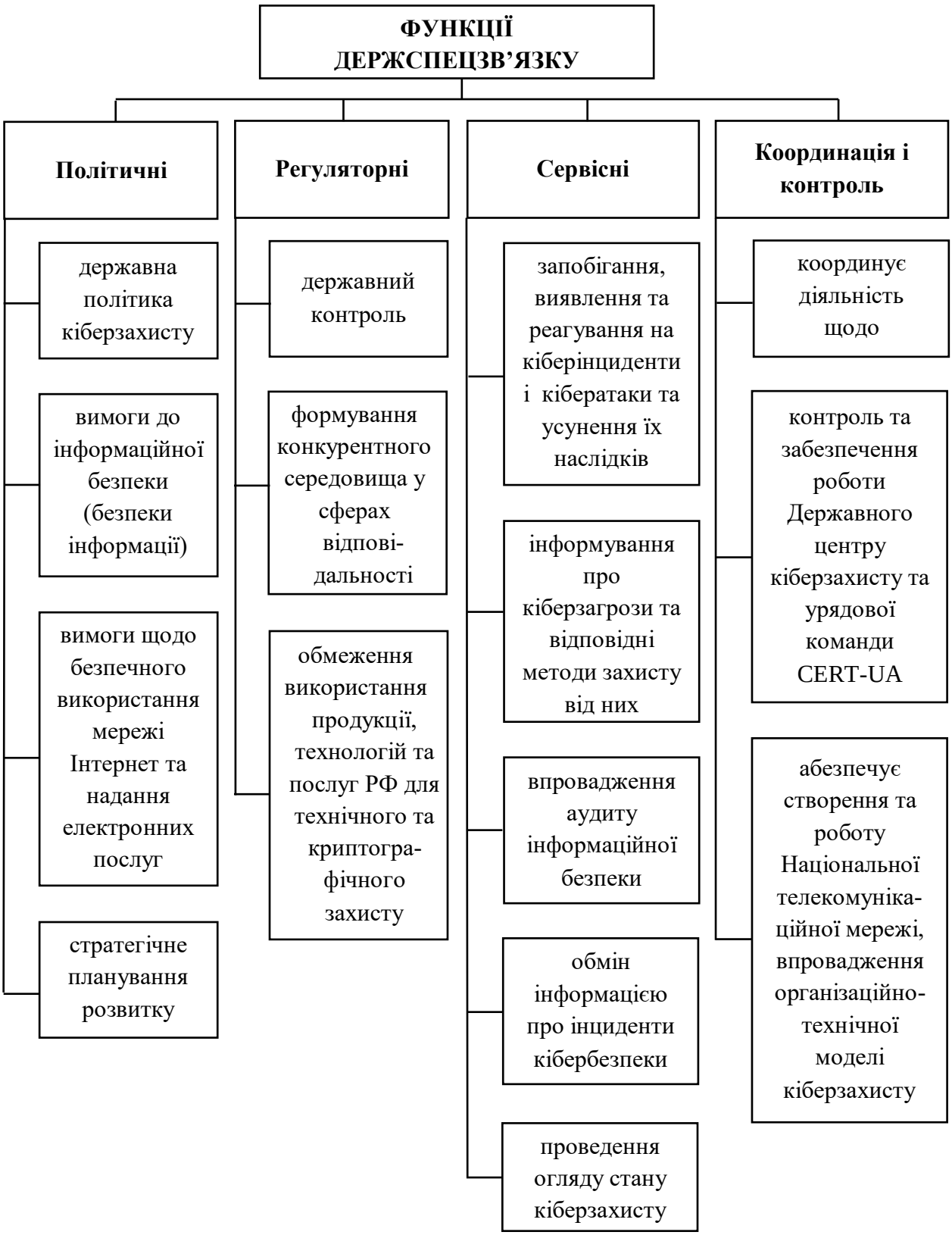
3. Звіт про роботу Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/services/cm/api/attachment/download? id=53656%20.

Додаток Б



Місце та роль кіберзахисту у забезпеченні кібербезпеки

Додаток В



Функції Держспецзв'язку як органу із забезпечення формування та реалізації державної політики

Додаток Г

Комплекс заходів з безпечного функціонування кіберпростору

Додаток Д

Огляд стану кіберзахисту в організаційно-правовому механізмі комплексного огляду сектору безпеки і оборони

Додаток Е

Матриця державного партнерства