МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ
Кафедра політології та публічного управління

На правах рукопису

МАРЧАК ЯНА ВАСИЛІВНА

Особливості, механізми та напрями вдосконалення діяльності силових структур із захисту кіберпростору України в умовах повномасштабної війни

Спеціальність 281 «Публічне управління та адміністрування»
Освітньо-професійна програма «Державна служба»
Робота на здобуття освітнього ступеня «Магістр»

Науковий керівник:
Панишко Галина Тарасівна,
кан. іст. наук, доцент

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол №
засідання кафедри політології
та публічного управління
від « » 2024 р.
Завідувач кафедри
Бусленко В. В. _____

ЛУЦЬК – 2024

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Повномасштабне вторгнення Російської Федерації в Україну започаткувало новий етап протистояння у кіберпросторі, масштаби та інтенсивність якого не мають історичних прецедентів. Кібератаки стали невід'ємною складовою військової агресії, демонструючи принципово нову якість гібридної війни, де цифрові технології використовуються для синхронізованого враження критичної інфраструктури, дестабілізації систем державного управління та порушення роботи об'єктів стратегічного значення. Трансформація характеру кіберзагроз виявляється у їх комплексності, коли технічні засоби кібератак поєднуються з методами соціальної інженерії, дезінформацією та психологічними операціями. Така конвергенція різних типів впливу створює мультиплікативний ефект, значно підвищуючи потенційну шкоду від кібератак. Силові структури України, які традиційно зосереджувались на протидії окремим видам кіберзагроз, стикаються з необхідністю кардинального перегляду усталених підходів до забезпечення кібербезпеки.

Особливого значення набуває проблематика міжвідомчої координації та синергії зусиль різних силових структур у протидії кіберзагрозам. Досвід перших місяців повномасштабної війни продемонстрував, що ізольовані дії окремих відомств не забезпечують належного рівня кіберзахисту в умовах масованих, добре скоординованих атак противника. Виникає нагальна потреба у формуванні єдиної системи реагування на кіберінциденти, що охоплюватиме усі рівні - від технічного виявлення загроз до стратегічного планування контрзаходів. Процеси діджиталізації державного управління, які значно прискорилися під час війни, створюють додаткові виклики для системи кібербезпеки.

Впровадження електронного документообігу, цифрових сервісів для громадян, автоматизованих систем управління військами підвищує залежність критично важливих процесів від надійності кіберзахисту. При цьому

традиційні методи забезпечення інформаційної безпеки часто виявляються неефективними проти новітніх кіберзагроз, що використовують штучний інтелект, квантові обчислення та інші передові технології. Досвід протистояння України російській агресії у кіберпросторі має унікальне значення для розвитку глобальної системи кібербезпеки. Вперше в історії відбувається масштабне застосування кіберзброї у поєднанні з конвенційними військовими діями, що дозволяє вивчити особливості такого комбінованого впливу та розробити ефективні механізми протидії. Аналіз діяльності силових структур України у цих безпрецедентних умовах може стати основою для формування нової парадигми кібербезпеки, адаптованої до реалій гібридної війни.

Теоретичне підґрунтя дослідження кібербезпеки сформували праці вітчизняних та зарубіжних науковців. Концептуальні засади кібербезпеки розглядали В. Бурячок, В. Петров, О. Корченко. Проблематику діяльності силових структур у кіберпросторі досліджували Д. Дубов, М. Погорецький, В. Шеломенцев. Правові аспекти забезпечення кібербезпеки висвітлювали І. Діордіца, В. Ліпкан, В. Шамрай. Технологічні аспекти кіберзахисту аналізували О. Юдін, С. Гнатюк, В. Хорошко. Міжнародний досвід протидії кіберзагрозам вивчали О. Баранов, В. Бутузов, В. Пилипчук.

Водночас, комплексне дослідження ролі силових структур у захисті кіберпростору України в умовах повномасштабної війни досі не проводилося. Потребують поглибленого аналізу механізми координації діяльності силових відомств, особливості протидії гібридним кіберзагрозам та напрями модернізації системи кіберзахисту з урахуванням набутого досвіду.

Мета і завдання дослідження. Метою роботи є комплексний аналіз діяльності силових структур України щодо захисту кіберпростору в умовах повномасштабної війни та розробка науково обґрунтованих рекомендацій з удосконалення системи кіберзахисту держави.

Для досягнення поставленої мети визначено **такі завдання:**

- систематизувати теоретико-методологічні засади дослідження кібербезпеки та діяльності силових структур у кіберпросторі;
- проаналізувати нормативно-правове забезпечення діяльності силових структур у сфері кібербезпеки;
- дослідити структуру та повноваження основних суб'єктів забезпечення кібербезпеки України;
- визначити особливості взаємодії силових структур у протидії кіберзагрозам в умовах війни;
- виявити основні виклики та загрози у кіберпросторі України під час повномасштабної війни;
- розробити рекомендації щодо вдосконалення діяльності силових структур із захисту кіберпростору України.

Об'єкт дослідження – діяльність силових структур України щодо забезпечення кібербезпеки держави.

Предмет дослідження – особливості, механізми та напрями вдосконалення діяльності силових структур із захисту кіберпростору України в умовах повномасштабної війни.

Методи дослідження. Методологічну основу роботи становить комплексний міждисциплінарний підхід. Використано загальнонаукові методи аналізу, синтезу, систематизації, порівняння та узагальнення. Застосовано системний підхід для дослідження взаємозв'язків між суб'єктами забезпечення кібербезпеки, інституційний метод – для аналізу нормативно-правової бази, структурно-функціональний – для вивчення розподілу повноважень між силовими структурами. Емпіричну базу склали методи експертного опитування, аналізу документів та case-study.

Наукова новизна одержаних результатів полягає в тому, що вперше здійснено комплексне дослідження діяльності силових структур України щодо захисту кіберпростору в умовах повномасштабної війни. Удосконалено теоретико-методологічні підходи до аналізу системи кібербезпеки держави.

Набули подальшого розвитку наукові положення щодо механізмів координації діяльності силових структур у кіберпросторі.

Практичне значення одержаних результатів полягає в можливості використання теоретичних положень та практичних рекомендацій для вдосконалення діяльності силових структур із захисту кіберпростору України. Результати дослідження можуть бути використані при розробці нормативно-правових актів, навчальних програм та методичних матеріалів.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Поняття кіберпростору та кібербезпеки у сучасній науці

Кіберпростір становить унікальне середовище функціонування суспільства, характеризується відсутністю кордонів та динамічним розвитком інформаційних технологій. За визначенням Дубова Д. В. кіберпростір являє собою специфічне середовище, яке виникає внаслідок функціонування інформаційних систем та мереж, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори й контролери [31]. Формування понятійного апарату у сфері кіберпростору відображає складність та багатовимірність досліджуваного явища. Мельник С. В., Тихомиров О. О., Лєнков О. С. розглядають кіберпростір як сферу існування цифрової форми представлення інформації, що формується, змінюється в результаті процесів інформаційної взаємодії [45]. Даник Ю. Г., Воробієнко П. П., Чернега В. М. акцентують увагу на технологічній природі кіберпростору, визначаючи його як простір, сформований інформаційно-комунікаційними системами, в якому проходять процеси перетворення цифрової інформації [17].

Структурні елементи кіберпростору охоплюють інформаційні ресурси, інформаційну інфраструктуру, суб'єктів інформаційної взаємодії. Грищук Р. В. та Даник Ю. Г. виділяють у структурі кіберпростору технологічну, інформаційну, комунікативну складові [15]. Технологічна складова представлена апаратно-програмними комплексами, телекомунікаційними мережами та системами. Інформаційна складова включає дані, інформаційні ресурси та процеси їх обробки. Комунікативна складова охоплює соціальні взаємодії та відносини між суб'єктами кіберпростору. Розвиток кіберпростору супроводжується виникненням нових загроз та викликів національній безпеці

держави. Довгань О. Д. та Доронін І. М. наголошують на зростанні кількості та складності кіберзагроз, спрямованих на порушення функціонування критичної інформаційної інфраструктури держави [28]. Бурячок В. Л. підкреслює необхідність формування комплексної системи кібернетичної безпеки для протидії деструктивним впливам у кіберпросторі [4]. Трансформація кіберпростору призводить до появи нових форм протиборства між державами. Діордіца І. В. розглядає кібершпигунство як загрозу національним інтересам держави в умовах геополітичного протистояння [26]. Ткачук Т. Ю. наголошує на необхідності вдосконалення правових механізмів забезпечення інформаційної безпеки держави в кіберпросторі [52]. Функціонування кіберпростору нерозривно пов'язане з розвитком інформаційних технологій та формуванням глобального інформаційного суспільства. Юдін О. К. розглядає інформаційну безпеку як невід'ємну складову національної безпеки держави в умовах інформатизації суспільства [60]. Корченко О. Г. наголошує на необхідності розробки ефективних механізмів протидії кібератакам для захисту національних інтересів у кіберпросторі [40].

Розвиток системи кібербезпеки потребує налагодження ефективної взаємодії між державним та приватним секторами. Марушак А. та Панченко В. підкреслюють необхідність впровадження механізмів державно-приватного партнерства у сфері забезпечення кібербезпеки [44]. Трофименко О. Г. наголошує на важливості вдосконалення нормативно-правової бази для регулювання відносин у сфері кібербезпеки [54].

Сучасні тенденції розвитку кіберпростору характеризуються посиленням впливу інформаційних технологій на всі сфери суспільного життя. Безуглий Д. визначає інформаційну безпеку як ключовий фактор забезпечення національних інтересів держави в умовах цифрової трансформації суспільства [2]. Світлична В. Ю. та Світлична Т. І. підкреслюють багатоаспектність проблеми забезпечення інформаційної безпеки та необхідність комплексного підходу до протидії кіберзагрозам [49].

Формування концепції кібербезпеки відбувалося паралельно з розвитком інформаційних технологій та становленням глобального інформаційного суспільства. Трансформація підходів до розуміння кібербезпеки відображає еволюцію загроз та викликів у кіберпросторі. На початковому етапі кібербезпека розглядалася переважно як технічний аспект захисту інформації в комп'ютерних системах та мережах [39]. Розвиток мережі Інтернет та поширення інформаційно-комунікаційних технологій зумовили розширення змісту поняття кібербезпеки. Поступово сформувалося розуміння кібербезпеки як комплексного явища, що охоплює технічні, організаційні, правові та соціальні аспекти захисту кіберпростору [54]. Становлення інформаційного суспільства супроводжувалося усвідомленням критичної ролі кібербезпеки для забезпечення національних інтересів держави [31].

Таблиця 1.1

Еволюція наукових підходів до визначення поняття кібербезпеки

Період	Характеристика підходу	Ключові аспекти
1990-2000	Технократичний	Захист комп'ютерних систем та мереж [35]
2001-2010	Комплексний	Інтеграція технічних та організаційних заходів [3]
2011-2020	Стратегічний	Забезпечення національних інтересів у кіберпросторі [47]
2021-теп.час	Інтегрований	Поєднання кібербезпеки з іншими видами безпеки [17]

Джерело: *складено автором на основі [37]*

Сучасне трактування кібербезпеки характеризується багатовимірністю та міждисциплінарністю. Інтеграція різних аспектів забезпечення безпеки в кіберпросторі знайшла відображення в нормативно-правових документах та наукових дослідженнях [48]. Концептуальні засади кібербезпеки охоплюють захист критичної інформаційної інфраструктури, протидію кіберзлочинності, забезпечення конфіденційності інформації [7].

Методологічні підходи до дослідження кібербезпеки зазнали суттєвої трансформації. Від вузькотехнічного розуміння відбувся перехід до системного аналізу проблем забезпечення безпеки в кіберпросторі. Формування національних систем кібербезпеки супроводжується розвитком

теоретико-методологічних засад дослідження механізмів протидії кіберзагрозам [32].

Становлення кібербезпеки як наукової категорії відбувалося в контексті розвитку інформаційного суспільства та цифрової економіки. Розширення спектру загроз у кіберпросторі зумовило необхідність розробки нових підходів до забезпечення безпеки інформаційних ресурсів та інфраструктури [28]. Інтеграція України до європейського кіберпростору актуалізувала питання гармонізації національного законодавства з міжнародними стандартами у сфері кібербезпеки [10]. Еволюція наукових поглядів на кібербезпеку супроводжується формуванням нових напрямів досліджень. Розвиток технологій штучного інтелекту та машинного навчання створює передумови для вдосконалення систем виявлення та протидії кіберзагрозам [40]. Впровадження технологій блокчейн відкриває нові можливості для забезпечення цілісності та достовірності інформації в кіберпросторі [56].

Глобалізація інформаційних процесів зумовлює необхідність міжнародного співробітництва у сфері кібербезпеки. Формування механізмів колективної безпеки в кіберпросторі стає пріоритетним напрямом розвитку систем захисту національних інтересів [44]. Державно-приватне партнерство розглядається як ефективний інструмент забезпечення кібербезпеки в умовах зростання складності та масштабності кіберзагроз [55].

Стрімкий розвиток інформаційних технологій супроводжується появою нових форм деструктивного впливу в кіберпросторі. Масштабні кібератаки на об'єкти критичної інфраструктури демонструють зростання рівня технологічної складності та руйнівного потенціалу кіберзагроз. Інтеграція кіберпростору в усі сфери життєдіяльності суспільства створює передумови для використання кібератак як інструменту геополітичного протистояння [25]. Природа сучасних кіберзагроз характеризується комплексністю та багатовекторністю впливу на інформаційні системи. Кібершпигунство набуває промислових масштабів, створюючи загрози національній безпеці та економічному розвитку держави. Методи соціальної інженерії

використовуються для отримання несанкціонованого доступу до конфіденційної інформації та критично важливих систем управління. Поширення технологій штучного інтелекту відкриває нові можливості для автоматизації процесів виявлення вразливостей та проведення кібератак [38].

Трансформація характеру кіберзагроз зумовлює необхідність розвитку систем кіберзахисту та вдосконалення механізмів протидії деструктивним впливам у кіберпросторі. Зростання кількості інцидентів кібербезпеки свідчить про необхідність впровадження проактивних методів захисту інформаційних ресурсів та інфраструктури. Розвиток технологій розподілених обчислень та Інтернету речей створює нові вектори кібератак, що потребують розробки інноваційних підходів до забезпечення кібербезпеки [12].

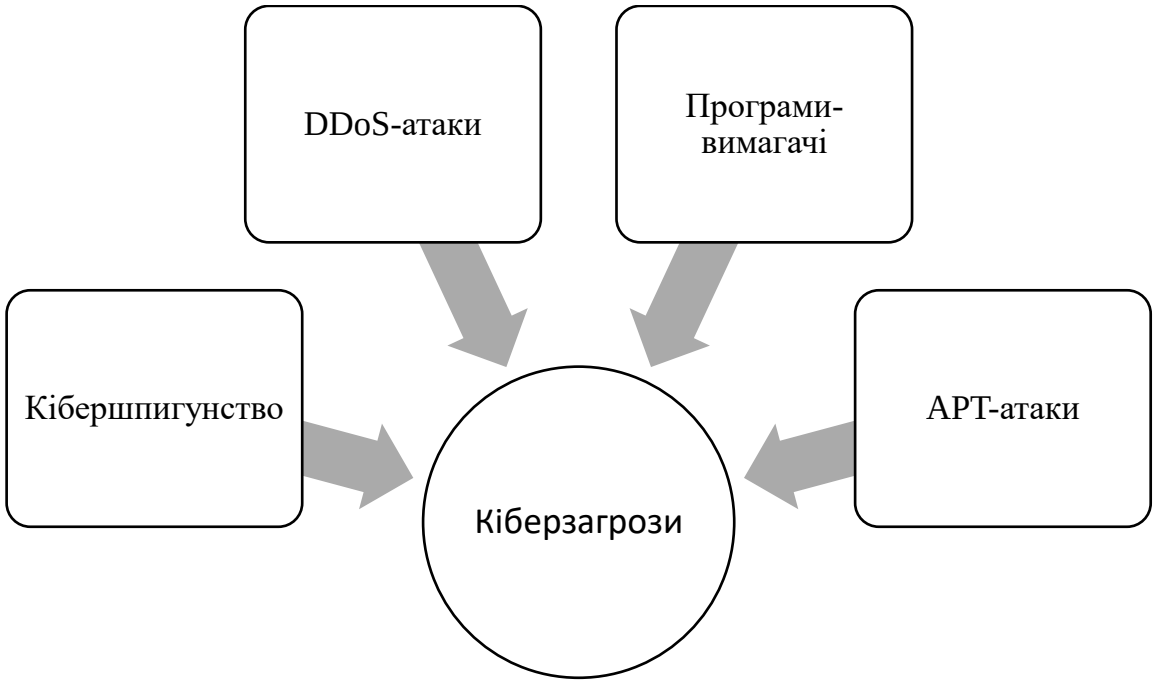

Рис. 1.2 Класифікація основних типів кіберзагроз

Джерело: *складено автором на основі [25]*

Масштабування кіберзагроз відбувається на фоні розвитку технологій хмарних обчислень та мобільного зв'язку. Методи проведення кібератак постійно вдосконалюються, що ускладнює процес виявлення та нейтралізації загроз. Зростання рівня автоматизації виробничих процесів створює передумови для порушення функціонування промислових систем управління

через кібератаки. Формування ефективної системи протидії кіберзагрозам потребує налагодження міжнародного співробітництва та обміну інформацією про інциденти кібербезпеки. Кіберзлочинність набуває транснаціонального характеру, що зумовлює необхідність координації зусиль правоохоронних органів різних держав. Розвиток механізмів державно-приватного партнерства розглядається як перспективний напрям підвищення рівня захищеності критичної інформаційної інфраструктури [57].

Протидія кіберзагрозам вимагає постійного моніторингу та аналізу тенденцій розвитку інформаційних технологій. Розробка методів прогнозування та попередження кібератак стає пріоритетним напрямом досліджень у сфері кібербезпеки. Впровадження технологій машинного навчання дозволяє автоматизувати процеси виявлення аномальної активності в інформаційних системах та мережах. Специфіка сучасних кіберзагроз полягає у поєднанні технічних та соціальних методів впливу на інформаційні системи. Атаки на ланцюги поставок програмного забезпечення демонструють зростання складності та масштабності кіберзагроз. Використання методів соціальної інженерії та психологічного впливу створює додаткові виклики для систем забезпечення кібербезпеки [34]. Національна система кібербезпеки включає широкий спектр суб'єктів, наділених повноваженнями щодо забезпечення безпеки кіберпростору. Законодавство України визначає повноваження та функції державних органів у сфері кібербезпеки, встановлює механізми координації їх діяльності. Регулювання відносин у сфері кібербезпеки здійснюється з урахуванням необхідності забезпечення балансу між інтересами особи, суспільства та держави [47].

Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України реалізують державну політику у сфері кібербезпеки відповідно до своєї компетенції. Розмежування повноважень між суб'єктами забезпечення кібербезпеки створює передумови для формування ефективної системи захисту національних інтересів у кіберпросторі.

Координація діяльності суб'єктів забезпечення кібербезпеки здійснюється через Національний координаційний центр кібербезпеки.

Державні органи у сфері кібербезпеки забезпечують моніторинг кіберпростору з метою своєчасного виявлення та запобігання кіберзагрозам, здійснюють розслідування кіберінцидентів та кібератак, забезпечують захист об'єктів критичної інформаційної інфраструктури. Інтеграція зусиль різних відомств дозволяє створити комплексну систему протидії кіберзагрозам та мінімізувати потенційні збитки від кібератак [53].

Об'єкти кібербезпеки охоплюють конституційні права і свободи громадян, системи електронних комунікацій, об'єкти критичної інформаційної інфраструктури, інформаційні ресурси держави. Забезпечення безпеки об'єктів кіберзахисту потребує впровадження комплексних систем захисту інформації, проведення аудиту інформаційної безпеки, розробки планів відновлення після кіберінцидентів. Правоохоронні органи здійснюють досудове розслідування кіберзлочинів, забезпечують збір та фіксацію доказів вчинення правопорушень у кіберпросторі, проводять експертні дослідження комп'ютерних систем та даних. Ефективність протидії кіберзлочинності значною мірою залежить від рівня міжвідомчої взаємодії та налагодження міжнародного співробітництва у сфері кібербезпеки [36].

Науково-дослідні установи та заклади вищої освіти забезпечують наукове супроводження діяльності у сфері кібербезпеки, здійснюють підготовку фахівців з кібербезпеки, проводять наукові дослідження проблем забезпечення кібербезпеки. Розвиток наукового потенціалу створює передумови для розробки інноваційних методів та засобів захисту кіберпростору. Впровадження результатів наукових досліджень сприяє підвищенню ефективності систем кіберзахисту. Підприємства, установи та організації, які провадять діяльність, пов'язану із забезпеченням кібербезпеки, здійснюють захист власних інформаційних ресурсів та інфраструктури, впроваджують системи управління інформаційною безпекою, проводять навчання персоналу з питань кібербезпеки. Розвиток державно-приватного партнерства у сфері

кібербезпеки дозволяє об'єднати ресурси держави та бізнесу для протидії кіберзагрозам [24].

Громадяни України, громадські об'єднання та організації беруть участь у формуванні та реалізації державної політики у сфері кібербезпеки, здійснюють громадський контроль за діяльністю суб'єктів забезпечення кібербезпеки. Підвищення рівня обізнаності громадян щодо кіберзагроз та методів захисту в кіберпросторі сприяє формуванню культури кібербезпеки в суспільстві. Методологічні засади забезпечення кібербезпеки ґрунтуються на системному підході до аналізу загроз та вразливостей у кіберпросторі. Формування концептуальних підходів відбувається з урахуванням динамічного характеру кіберзагроз та необхідності постійної адаптації механізмів захисту. Системний підхід передбачає комплексне врахування технічних, організаційних, правових та соціальних аспектів забезпечення кібербезпеки. Стратегічне планування у сфері кібербезпеки здійснюється на основі аналізу тенденцій розвитку інформаційних технологій та прогнозування потенційних загроз [15]. Технологічний підхід до забезпечення кібербезпеки базується на впровадженні сучасних засобів захисту інформації та систем виявлення вторгнень. Розвиток технологій штучного інтелекту та машинного навчання створює нові можливості для автоматизації процесів моніторингу та реагування на кіберінциденти. Архітектура систем кіберзахисту будується за принципом багаторівневого захисту, що дозволяє забезпечити стійкість до різних типів кібератак. Впровадження технологій блокчейн розглядається як перспективний напрям підвищення надійності систем ідентифікації та автентифікації користувачів [31].

Організаційний підхід зосереджується на формуванні ефективної структури управління кібербезпекою та налагодженні взаємодії між різними підрозділами. Розподіл відповідальності та повноважень між суб'єктами забезпечення кібербезпеки здійснюється відповідно до їх компетенції та функціональних обов'язків. Процесний підхід до управління кібербезпекою передбачає стандартизацію процедур реагування на інциденти та

впровадження систем управління безперервністю бізнесу. Розвиток механізмів координації та обміну інформацією сприяє підвищенню ефективності протидії кіберзагрозам [42].

Правовий підхід забезпечує нормативне регулювання відносин у сфері кібербезпеки та встановлює відповідальність за порушення вимог законодавства. Гармонізація національного законодавства з міжнародними стандартами створює передумови для розвитку міжнародного співробітництва у сфері кібербезпеки. Формування правових механізмів захисту критичної інформаційної інфраструктури відбувається з урахуванням міжнародного досвіду та національних особливостей. Впровадження механізмів сертифікації та стандартизації у сфері кібербезпеки сприяє підвищенню рівня довіри до інформаційних систем та послуг [54].

Ризик-орієнтований підхід передбачає оцінку ймовірності реалізації загроз та потенційного збитку від кібератак. Методологія управління ризиками кібербезпеки базується на систематичному аналізі вразливостей та розробці заходів з мінімізації ризиків. Впровадження систем управління інформаційною безпекою здійснюється на основі оцінки ризиків та визначення пріоритетів захисту. Розвиток методів кількісної оцінки ризиків дозволяє обґрунтувати інвестиції в системи кіберзахисту [5]. Компетентнісний підхід зосереджується на розвитку людського потенціалу та формуванні необхідних навичок у сфері кібербезпеки. Підготовка фахівців з кібербезпеки здійснюється з урахуванням сучасних вимог та тенденцій розвитку інформаційних технологій. Впровадження програм підвищення кваліфікації та сертифікації персоналу сприяє підвищенню рівня професійної компетентності фахівців з кібербезпеки. Формування культури кібербезпеки в організації розглядається як ключовий елемент системи захисту інформації [28].

Проактивний підхід до забезпечення кібербезпеки передбачає випереджальне виявлення та усунення вразливостей інформаційних систем. Розвиток систем раннього попередження про кіберзагрози дозволяє мінімізувати ризики успішної реалізації кібератак. Впровадження технологій

поведінкового аналізу та аномалій мережевого трафіку створює можливості для виявлення прихованих загроз. Постійний моніторинг кіберпростору та аналіз тенденцій розвитку кіберзагроз забезпечує актуалізацію механізмів захисту [40]. Інтегрований підхід до забезпечення кібербезпеки поєднує різні методи та засоби захисту інформації в єдину систему. Координація зусиль різних підрозділів та організацій здійснюється на основі єдиних принципів та стандартів безпеки. Розвиток державно-приватного партнерства у сфері кібербезпеки створює синергетичний ефект від об'єднання ресурсів та компетенцій. Формування екосистеми кібербезпеки на національному рівні забезпечує стійкість до сучасних викликів та загроз.

Методологія дослідження ролі силових структур у захисті кіберпростору

Методологічний інструментарій дослідження ролі силових структур у захисті кіберпростору базується на фундаментальних загальнонаукових принципах та методах пізнання. Методологічна основа наукового пошуку формується з урахуванням специфіки предметного поля кібербезпеки та особливостей функціонування державних силових структур в умовах повномасштабної війни. Застосування системного підходу дозволяє розглядати кіберпростір як складну динамічну систему, що характеризується множинністю елементів та взаємозв'язків між ними [1].

Діалектичний метод наукового пізнання розкриває сутність кібербезпекових процесів через єдність та боротьбу протилежностей, що проявляється у постійному протистоянні захисних механізмів та кіберзагроз. Структурно-функціональний аналіз забезпечує можливість декомпозиції системи кібербезпеки на складові елементи та дослідження функціональних зв'язків між ними. Застосування методу абстрагування дозволяє виокремити найбільш суттєві характеристики досліджуваних явищ та процесів у сфері кіберзахисту, відволікаючись від другорядних ознак та властивостей.

Синергетичний підхід розкриває механізми самоорганізації та саморозвитку системи кібербезпеки держави в умовах нелінійності та нестабільності зовнішнього середовища. Методи аналізу та синтезу застосовуються для декомпозиції складних явищ кіберпростору на простіші складові та подальшого об'єднання отриманих результатів у цілісну теоретичну конструкцію. Індуктивний та дедуктивний методи забезпечують можливість формулювання теоретичних узагальнень на основі емпіричних даних та практичної верифікації теоретичних положень [7].

Метод моделювання дозволяє створювати абстрактні моделі кіберзагроз та механізмів протидії ним, що має особливе значення в умовах швидкої зміни характеру кіберзагроз та необхідності превентивного реагування на них. Історичний метод застосовується для дослідження ґенези та еволюції системи кіберзахисту держави, що дає змогу виявити основні тенденції та закономірності її розвитку. Порівняльний метод створює підґрунтя для зіставлення різних підходів до організації кібербезпеки та виявлення найбільш ефективних практик [12].

Статистичний метод забезпечує можливість кількісного аналізу параметрів кіберзагроз та ефективності заходів протидії ним. Формально-логічний метод застосовується для побудови несуперечливої системи теоретичних положень та практичних рекомендацій щодо удосконалення системи кіберзахисту. Аксіологічний підхід дозволяє визначити ціннісні орієнтири та пріоритети у сфері забезпечення кібербезпеки держави. Прогностичний метод створює можливості для передбачення потенційних кіберзагроз та розробки превентивних заходів захисту. Метод експертних оцінок застосовується для отримання якісних характеристик досліджуваних явищ на основі узагальнення думок фахівців у сфері кібербезпеки. Системний аналіз кіберпростору як середовища протиборства потребує врахування множинності факторів впливу та складності взаємозв'язків між ними. Інституційний підхід дозволяє досліджувати формальні та неформальні норми, що регулюють діяльність суб'єктів у кіберпросторі. Структурний метод

застосовується для виявлення та аналізу стійких зв'язків між елементами системи кіберзахисту, що визначають її цілісність. Функціональний аналіз спрямований на дослідження способів реалізації функцій силових структур у сфері забезпечення кібербезпеки держави [23].

Спеціальні методи дослідження діяльності силових структур у сфері кібербезпеки характеризуються специфічною спрямованістю та унікальним інструментарієм, що враховує особливості функціонування правоохоронних органів та спецслужб в умовах гібридних загроз. Методологічний апарат включає сукупність взаємопов'язаних підходів, які дозволяють всебічно дослідити специфіку діяльності силових структур у кіберпросторі. Аналітико-прогностичний метод забезпечує можливість виявлення тенденцій розвитку кіберзагроз та формування превентивних механізмів захисту критичної інформаційної інфраструктури держави. Оперативно-тактичний метод розкриває особливості планування та реалізації заходів із протидії кіберзлочинності, враховуючи специфіку діяльності різних підрозділів силових структур. Метод сценарного моделювання дозволяє розробляти та аналізувати різні варіанти розвитку кризових ситуацій у кіберпросторі, формуючи відповідні алгоритми реагування. Ситуаційний аналіз застосовується для оцінки конкретних випадків кібератак та розробки механізмів протидії з урахуванням наявних ресурсів та можливостей силових структур. Метод кримінального профілювання використовується для створення психологічних портретів кіберзлочинців та прогнозування їхньої можливої поведінки. Криміналістичний аналіз цифрових слідів дозволяє встановлювати причинно-наслідкові зв'язки між різними кіберінцидентами та виявляти закономірності у діяльності зловмисників. Метод оперативного впровадження забезпечує можливість отримання інформації про підготовку кібератак з середини злочинних угруповань [11].

Контент-аналіз інформаційних потоків у кіберпросторі дозволяє виявляти потенційні загрози національній безпеці та вживати превентивних заходів. Метод кореляційного аналізу застосовується для встановлення взаємозв'язків

між різними проявами кіберзлочинності та факторами, що впливають на їх виникнення. Системно-динамічне моделювання забезпечує можливість дослідження процесів еволюції кіберзагроз та адаптації механізмів захисту. Метод мережевого аналізу розкриває структуру взаємозв'язків між суб'єктами кіберзлочинності та дозволяє виявляти ключові вузли злочинних мереж. Івент-аналіз застосовується для дослідження послідовності подій у кіберпросторі та встановлення закономірностей у діяльності зловмисників. Метод кластерного аналізу дозволяє групувати кіберінциденти за подібними характеристиками та розробляти типові алгоритми реагування. Метод форензічного аналізу цифрових даних забезпечує можливість отримання доказової бази щодо фактів кіберзлочинів. Просторово-часовий аналіз застосовується для виявлення географічних та часових закономірностей у здійсненні кібератак. Метод реконструкції кіберінцидентів дозволяє відтворювати послідовність дій зловмисників та механізми реалізації кібератак [25].

Операційний аналіз діяльності силових структур спрямований на оптимізацію використання наявних ресурсів та підвищення ефективності заходів із протидії кіберзагрозам. Метод компаративного аналізу дозволяє зіставляти ефективність різних підходів до організації кіберзахисту та виявляти найбільш результативні практики. Праксеологічний метод застосовується для дослідження практичного досвіду протидії кіберзлочинності та формування рекомендацій щодо удосконалення діяльності силових структур [29].

Міждисциплінарний підхід у дослідженні кібербезпеки розкриває комплексний характер проблематики захисту кіберпростору та необхідність інтеграції знань з різних наукових галузей. Поєднання методологічного інструментарію правових, технічних, соціальних, психологічних та управлінських наук створює фундаментальну основу для всебічного аналізу феномену кібербезпеки. Методологічна конвергенція різних наукових напрямів дозволяє формувати інноваційні підходи до розв'язання проблем захисту національного кіберпростору. Правова складова міждисциплінарного

підходу забезпечує дослідження нормативно-правового регулювання діяльності у кіберпросторі, механізмів притягнення до відповідальності за кіберзлочини, процедур міжнародного співробітництва у протидії кіберзагрозам. Технічні науки привносять інструментарій аналізу технологічних аспектів кібербезпеки, дослідження механізмів функціонування шкідливого програмного забезпечення, розробки систем захисту інформації. Соціологічні методи розкривають соціальну природу кіберзлочинності, досліджують вплив соціальних факторів на формування кіберзагроз, аналізують соціальні наслідки кібератак.

Психологічні методи дослідження дозволяють аналізувати поведінкові патерни кіберзлочинців, вивчати психологічні механізми соціальної інженерії, досліджувати психологічний вплив кібератак на суспільство. Управлінські науки забезпечують методологічну базу для дослідження процесів планування, організації та координації діяльності із забезпечення кібербезпеки, розробки механізмів прийняття рішень в умовах кіберзагроз, оцінки ефективності заходів кіберзахисту [9].

Економічні методи дослідження розкривають фінансові аспекти забезпечення кібербезпеки, аналізують економічні наслідки кібератак, досліджують механізми фінансування заходів кіберзахисту. Політологічний інструментарій застосовується для аналізу геополітичних аспектів кібербезпеки, дослідження явища кібертероризму, вивчення механізмів використання кіберпростору як середовища політичного протиборства. Методи криміналістики забезпечують можливість дослідження механізмів скоєння кіберзлочинів, збору та аналізу цифрових доказів, ідентифікації злочинців у кіберпросторі. Математичні методи створюють основу для моделювання процесів у кіберпросторі, прогнозування розвитку кіберзагроз, оцінки ризиків та розробки алгоритмів захисту. Філософський інструментарій дозволяє осмислити фундаментальні аспекти розвитку кіберпростору, етичні проблеми використання інформаційних технологій, питання відповідальності за дії у віртуальному середовищі. Методи педагогіки застосовуються для

дослідження процесів формування культури кібербезпеки, розробки освітніх програм з підготовки фахівців [14].

Лінгвістичні методи забезпечують можливість аналізу комунікативних аспектів кібербезпеки, дослідження механізмів інформаційного впливу через кіберпростір, вивчення особливостей спілкування в цифровому середовищі. Методи конфліктології розкривають природу протиборства у кіберпросторі, механізми ескалації кіберконфліктів, шляхи їх врегулювання. Культурологічний підхід дозволяє досліджувати вплив культурних факторів на формування кіберзагроз, особливості сприйняття кібербезпеки в різних культурних контекстах [18].

Міждисциплінарна синергія створює потужний методологічний базис для комплексного дослідження проблематики кібербезпеки. Інтеграція різних наукових підходів дозволяє формувати цілісне розуміння природи кіберзагроз та механізмів протидії їм. Методологічна конвергенція забезпечує можливість розробки ефективних стратегій захисту національного кіберпростору з урахуванням множинності факторів впливу [22]. Методики оцінки ефективності системи кіберзахисту базуються на комплексному підході до визначення здатності силових структур протистояти сучасним кіберзагрозам та забезпечувати належний рівень захисту критичної інформаційної інфраструктури держави. Комплексна оцінка включає аналіз технічних, організаційних, кадрових та фінансових аспектів функціонування системи кіберзахисту. Квантитативні методи оцінювання дозволяють отримати числові показники ефективності на основі математичного моделювання та статистичного аналізу даних про кіберінциденти [31].

Методологія оцінки вразливостей передбачає систематичне сканування інформаційних систем, виявлення потенційних точок проникнення, аналіз можливих векторів атак та оцінку потенційних збитків. Стрес-тестування систем захисту дозволяє визначити межі їх стійкості та виявити критичні точки відмови. Аналіз часу реагування на інциденти включає оцінку швидкості виявлення атак, прийняття рішень та впровадження контрзаходів.

Методика оцінки відновлюваності систем після кібератак враховує час простою, витрати на відновлення та повноту відновлення функціональності [34].

Кількісна оцінка ефективності базується на розрахунку ключових показників результативності, включаючи кількість відвернених атак, середній час виявлення загроз, відсоток успішно заблокованих спроб несанкціонованого доступу. Якісні методи оцінювання передбачають експертний аналіз відповідності систем захисту сучасним вимогам та стандартам кібербезпеки. Методика оцінки готовності персоналу включає тестування знань та навичок, проведення навчальних тривог, аналіз результатів протидії симульованим атакам [37].

Економічна ефективність системи кіберзахисту оцінюється через співвідношення витрат на забезпечення безпеки та потенційних збитків від кіберінцидентів. Методологія розрахунку return on security investment (ROSI) дозволяє визначити фінансову доцільність впровадження додаткових заходів захисту. Аналіз вартості володіння системами безпеки включає оцінку прямих та непрямих витрат на підтримку функціонування механізмів захисту [40].

Оцінка відповідності міжнародним стандартам передбачає порівняльний аналіз існуючих механізмів захисту з вимогами ISO/IEC 27001, NIST Cybersecurity Framework та інших загальновизнаних нормативів. Методика аудиту безпеки включає перевірку налаштувань систем захисту, аналіз політик безпеки, оцінку ефективності контрольних механізмів. Перевірка документації з кібербезпеки дозволяє оцінити повноту та актуальність регламентів, інструкцій та планів реагування на інциденти. Багатокритеріальна оцінка ефективності враховує множину параметрів, включаючи технічну досконалість систем захисту, кваліфікацію персоналу, швидкість реагування на інциденти, економічну ефективність заходів безпеки. Методика порівняльного аналізу дозволяє зіставити показники ефективності різних підрозділів та організацій, виявити кращі практики та напрями вдосконалення. Динамічна оцінка ефективності передбачає відстеження змін

показників захищеності в часі та виявлення тенденцій розвитку системи кіберзахисту. Методологія оцінки зрілості процесів кібербезпеки базується на моделях CMMI та дозволяє визначити рівень розвитку практик захисту інформації. Аналіз інцидентів включає дослідження причин успішних атак, оцінку адекватності вжитих заходів протидії, визначення напрямів удосконалення систем захисту. Прогностична оцінка ефективності передбачає моделювання майбутніх загроз та перевірку готовності систем захисту до протидії новим викликам [49].

Інтегральна оцінка ефективності системи кіберзахисту формується на основі зважених показників, що відображають різні аспекти забезпечення безпеки інформаційних активів. Методика оцінки синергетичного ефекту дозволяє визначити результативність взаємодії різних компонентів системи захисту. Оцінка адаптивності систем кіберзахисту включає аналіз здатності до швидкого реагування на зміни характеру загроз та впровадження нових механізмів протидії [52].

Висновки до розділу 1

1. Проведений теоретико-методологічний аналіз засвідчує багатовимірність та комплексність феномену кібербезпеки в умовах гібридної війни. На підставі систематизації наукових підходів встановлено, що кіберпростір як середовище діяльності силових структур характеризується специфічними властивостями: відсутністю географічних кордонів, асиметричністю загроз, складністю атрибуції кібератак та високою динамікою розвитку технологій. Дослідження еволюції концептуальних підходів до забезпечення кібербезпеки держави дозволило виявити трансформацію парадигми від суто технічного захисту інформації до комплексної системи протидії кіберзагрозам, що охоплює організаційні, правові, технологічні та освітні аспекти. Нормативно-правова база у сфері кібербезпеки України демонструє поступовий розвиток від фрагментарного регулювання окремих питань до формування цілісної системи правових норм, хоча все ще потребує

гармонізації з міжнародними стандартами та адаптації до сучасних викликів гібридної війни.

2. Методологічний інструментарій дослідження ролі силових структур у захисті кіберпростору характеризується міждисциплінарністю та інтеграцією різних наукових підходів. Застосування системного підходу дозволило розглянути кібербезпеку як складну соціотехнічну систему, де технологічні аспекти нерозривно пов'язані з людським фактором та організаційними процесами. Синергетична методологія уможливила дослідження процесів самоорганізації та емерджентних властивостей системи кіберзахисту в умовах нелінійності та невизначеності. Інституційний підхід забезпечив аналіз формальних та неформальних механізмів взаємодії силових структур, а структурно-функціональний метод дозволив виявити особливості розподілу повноважень та координації дій між різними відомствами. Емпіричну базу дослідження склали як кількісні показники кіберінцидентів та результативності протидії їм, так і якісний аналіз кейсів успішного реагування на кібератаки, що забезпечило всебічне висвітлення досліджуваної проблематики.

РОЗДІЛ 2
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР У СФЕРІ КІБЕРБЕЗПЕКИ

2.1 Міжнародне політико-правове регулювання діяльності силових структур у сфері кібербезпеки

В міжнародному правовому полі регулювання діяльності силових структур у сфері кібербезпеки базується на фундаментальних міжнародних документах, які формують основу для розбудови національних систем кіберзахисту. Будапештська конвенція про кіберзлочинність від 2001 року становить базовий міжнародний інструмент протидії кіберзагрозам, визначаючи основні види кіберзлочинів та механізми міжнародної співпраці в розслідуванні кіберінцидентів. Документ встановлює правові рамки для криміналізації протиправних дій у кіберпросторі, включаючи несанкціоноване втручання в роботу комп'ютерних систем, розповсюдження шкідливого програмного забезпечення та інші види кіберзлочинів.

Резолюції Генеральної Асамблеї ООН щодо кібербезпеки формують міжнародно-правову базу для захисту критичної інформаційної інфраструктури та протидії використанню інформаційно-комунікаційних технологій у злочинних цілях. Міжнародне співтовариство через механізми ООН розробило низку рекомендацій щодо забезпечення безпеки глобального кіберпростору, включаючи питання захисту персональних даних, безпеки електронної комерції та протидії кібертероризму. Нормативні документи НАТО у сфері кібербезпеки визначають стандарти та процедури реагування на кіберзагрози, механізми обміну інформацією про кіберінциденти між державами-членами альянсу. Політика кіберзахисту НАТО передбачає створення спільних центрів реагування на кіберзагрози, проведення навчань з кібербезпеки та розвиток спроможностей національних силових структур у протидії кібератакам. Регламенти та директиви Європейського Союзу

встановлюють єдині підходи до забезпечення кібербезпеки в європейському просторі. Директива NIS (Network and Information Security) визначає вимоги до захисту мережевої та інформаційної безпеки, зобов'язання операторів критичної інфраструктури щодо забезпечення кіберзахисту. Загальний регламент про захист даних (GDPR) встановлює правила обробки персональних даних та відповідальність за порушення вимог інформаційної безпеки.

Міжнародні угоди про взаємну правову допомогу у кримінальних справах забезпечують правову основу для співпраці силових структур різних держав у розслідуванні кіберзлочинів. Механізми міжнародної правової допомоги дозволяють здійснювати обмін доказами, проводити спільні розслідування та переслідувати кіберзлочинців незалежно від їх географічного місцезнаходження. Багатосторонні угоди про співробітництво в боротьбі з кіберзлочинністю визначають порядок взаємодії правоохоронних органів різних держав, механізми обміну оперативною інформацією та проведення спільних операцій. Міжнародне співробітництво силових структур включає створення спільних слідчих груп, проведення транскордонних операцій та обмін досвідом у протидії новим видам кіберзагроз.

Документи Міжнародного союзу електрозв'язку встановлюють технічні стандарти безпеки телекомунікаційних мереж та систем, процедури реагування на кіберінциденти в телекомунікаційному секторі. Рекомендації МСЕ охоплюють питання захисту телекомунікаційної інфраструктури від кібератак, забезпечення стійкості мереж зв'язку та безпеки послуг електрозв'язку. Міжнародні стандарти у сфері кібербезпеки серії ISO/IEC 27000 визначають вимоги до систем управління інформаційною безпекою, методології оцінки ризиків та заходи захисту інформаційних активів. Стандартизація підходів до забезпечення кібербезпеки сприяє підвищенню ефективності захисту інформаційних систем та міжнародній співпраці у протидії кіберзагрозам.

Регіональні угоди про співробітництво у сфері кібербезпеки створюють механізми взаємодії силових структур на регіональному рівні, включаючи обмін інформацією про кіберзагрози, проведення спільних навчань та розвиток спільних центрів реагування на кіберінциденти. Регіональне співробітництво дозволяє більш ефективно протидіяти транскордонним кіберзагрозам та розвивати спільні спроможності у сфері кіберзахисту. Міжнародно-правове регулювання сфери кібербезпеки характеризується багаторівневою структурою та охоплює широкий спектр нормативних документів різної юридичної сили. Базовим міжнародним документом у сфері протидії кіберзлочинності залишається Будапештська конвенція про кіберзлочинність від 2001 року, яка встановлює основні стандарти криміналізації правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем [15, 28].

Міжнародна спільнота через механізми ООН сформувала комплексний підхід до забезпечення кібербезпеки, що відображено у численних резолюціях Генеральної Асамблеї. Фундаментальні принципи міжнародного співробітництва у сфері кібербезпеки закладені в резолюціях, спрямованих на створення глобальної культури кібербезпеки та захисту критичної інформаційної інфраструктури [31, 32]. Нормативна база НАТО з питань кібербезпеки охоплює широкий спектр документів, включаючи політику кіберзахисту, концептуальні документи та технічні стандарти. Стратегічна концепція кібербезпеки НАТО передбачає розвиток колективних спроможностей протидії кіберзагрозам, проведення спільних навчань та обмін інформацією між державами-членами [44, 45].

Законодавство Європейського Союзу у сфері кібербезпеки формує комплексну систему захисту мережевої та інформаційної інфраструктури. Директива NIS встановлює мінімальні вимоги до національних систем кібербезпеки держав-членів ЄС, механізми транскордонного співробітництва та обміну інформацією про кіберінциденти [10, 24].

Міжнародні стандарти серії ISO/IEC 27000 складають технічну основу для побудови систем управління інформаційною безпекою. Стандартизація підходів до забезпечення кібербезпеки сприяє гармонізації національних систем захисту інформації та підвищенню ефективності міжнародного співробітництва у протидії кіберзагрозам [4, 13]. Регіональні механізми забезпечення кібербезпеки доповнюють глобальну систему міжнародно-правового регулювання. Регіональні угоди про співробітництво у сфері кібербезпеки створюють додаткові інструменти взаємодії силових структур, включаючи обмін інформацією про кіберзагрози та проведення спільних операцій [17, 28].

Міжнародні угоди про взаємну правову допомогу забезпечують правову основу для транскордонного розслідування кіберзлочинів. Механізми міжнародної правової допомоги дозволяють здійснювати обмін доказами, проводити спільні слідчі дії та забезпечувати невідворотність покарання кіберзлочинців незалежно від їх місцезнаходження. Документи Міжнародного союзу електрозв'язку встановлюють технічні стандарти безпеки телекомунікаційних мереж та процедури реагування на кіберінциденти у телекомунікаційному секторі. Рекомендації МСЕ охоплюють питання захисту телекомунікаційної інфраструктури від кібератак та забезпечення стійкості мереж зв'язку.

Багатосторонні угоди про співробітництво у боротьбі з кіберзлочинністю визначають порядок взаємодії правоохоронних органів різних держав, механізми обміну оперативною інформацією та проведення спільних операцій. Міжнародне співробітництво силових структур включає створення спільних слідчих груп, проведення транскордонних операцій та обмін досвідом у протидії новим видам кіберзагроз [28, 33].

Формування національної системи кібербезпеки відбувається з урахуванням міжнародних зобов'язань держави та передового досвіду провідних країн світу. Імплементація міжнародних стандартів та найкращих практик забезпечення кібербезпеки сприяє підвищенню ефективності

діяльності силових структур у протидії сучасним викликам та загрозам у кіберпросторі [47, 48].

2.2. Законодавство держави Україна

Конституційно-правові засади забезпечення кібербезпеки України базуються на фундаментальних положеннях Основного Закону держави, який визначає пріоритетність захисту національних інтересів у інформаційній сфері та кіберпросторі. Конституція України закріплює основоположні права громадян на інформацію, захист персональних даних та приватності у цифровому середовищі, встановлює обов'язки держави щодо забезпечення інформаційної безпеки як складової національної безпеки України [38].

Законодавче регулювання сфери кібербезпеки охоплює широкий спектр нормативно-правових актів різної юридичної сили, які формують комплексну систему правового забезпечення діяльності суб'єктів національної системи кібербезпеки. Ключові засади державної політики у сфері кібербезпеки визначені Законом України «Про основні засади забезпечення кібербезпеки України», який встановлює основні принципи, напрями та механізми державного регулювання у сфері кібербезпеки [7]. Стратегія кібербезпеки України як документ довгострокового планування визначає пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційні кіберзагрози, цілі та завдання забезпечення кібербезпеки України. Нормативно-правове підґрунтя діяльності суб'єктів забезпечення кібербезпеки формується з урахуванням необхідності створення умов для безпечного функціонування кіберпростору та його використання в інтересах суспільства [15].

Розвиток національного законодавства у сфері кібербезпеки відбувається з урахуванням динамічного характеру кіберзагроз та необхідності адаптації правових механізмів до нових викликів у кіберпросторі. Правове регулювання

діяльності суб'єктів забезпечення кібербезпеки спрямоване на створення ефективних механізмів протидії кіберзлочинності, кібертероризму та іншим проявам протиправної діяльності у кіберпросторі [28].

Нормативно-правове забезпечення функціонування національної системи кібербезпеки передбачає чітке розмежування повноважень та відповідальності між суб'єктами забезпечення кібербезпеки, визначення механізмів координації їх діяльності та порядку взаємодії під час реагування на кіберінциденти та кібератаки. Система правового регулювання охоплює питання захисту об'єктів критичної інформаційної інфраструктури, забезпечення кібербезпеки державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [44]. Правові механізми державно-приватного партнерства у сфері кібербезпеки створюють основу для залучення потенціалу приватного сектору до вирішення завдань кіберзахисту. Законодавче регулювання взаємодії державного та приватного секторів спрямоване на підвищення ефективності системи кібербезпеки через об'єднання ресурсів та можливостей усіх зацікавлених сторін. Нормативно-правове регулювання питань підготовки фахівців з кібербезпеки, проведення наукових досліджень та розробок у сфері кібербезпеки спрямоване на розвиток кадрового та наукового потенціалу національної системи кібербезпеки. Правові механізми стимулювання розвитку індустрії кібербезпеки створюють умови для впровадження сучасних технологій та рішень у сфері кіберзахисту [52].

Правове забезпечення міжнародного співробітництва у сфері кібербезпеки базується на міжнародних договорах України та створює правові механізми для участі національних суб'єктів забезпечення кібербезпеки у міжнародних ініціативах та проектах. Розвиток правової бази міжнародного співробітництва спрямований на посилення спроможностей України у протидії транскордонним кіберзагрозам [60].

Законодавче регулювання діяльності силових структур у кіберпросторі характеризується системним підходом до визначення правових засад функціонування суб'єктів сектору безпеки і оборони в умовах протидії

кіберзагрозам. Правове поле діяльності силових структур формується на основі конституційних норм та спеціального законодавства у сфері кібербезпеки, яке визначає компетенцію, повноваження та механізми взаємодії правоохоронних органів, спеціальних служб та військових формувань під час виконання завдань із забезпечення кібербезпеки держави. Нормативно-правова база охоплює питання організації оперативно-розшукової діяльності, проведення контррозвідувальних заходів та здійснення розвідувальної діяльності у кіберпросторі [15, 27].

Правове регулювання діяльності підрозділів кіберполіції спрямоване на забезпечення ефективної протидії кіберзлочинності та розслідування кримінальних правопорушень, вчинених з використанням інформаційних технологій. Законодавство визначає процесуальні аспекти збору та фіксації цифрових доказів, проведення комп'ютерно-технічних експертиз та інших слідчих дій у кіберпросторі. Регламентація оперативно-розшукових заходів у кіберпросторі враховує специфіку роботи правоохоронних органів в умовах використання новітніх інформаційних технологій та необхідність дотримання прав і свобод громадян при здійсненні правоохоронної діяльності [31, 32].

Правові механізми забезпечення кібероборони держави передбачають визначення повноважень військових формувань та спеціальних служб щодо захисту суверенітету держави у кіберпросторі. Законодавство встановлює порядок застосування сил та засобів сектору безпеки і оборони для протидії кібератакам, кібертероризму та іншим проявам агресії у кіберпросторі. Нормативно-правове регулювання охоплює питання створення та функціонування системи ситуаційних центрів, центрів реагування на кіберінциденти та інших спеціалізованих підрозділів силових структур [4, 17].

Правове забезпечення розвідувальної діяльності у кіберпросторі базується на спеціальному законодавстві, яке визначає правові підстави та порядок здійснення розвідувальних заходів з використанням технічних засобів. Законодавче регулювання діяльності розвідувальних органів враховує необхідність протидії розвідувально-підривній діяльності іноземних

спецслужб у кіберпросторі та забезпечення інформаційної переваги в умовах гібридних загроз. Нормативна база охоплює питання міжнародного співробітництва розвідувальних органів у сфері обміну інформацією про кіберзагрози та проведення спільних операцій. Законодавче регулювання захисту критичної інформаційної інфраструктури визначає роль та місце силових структур у забезпеченні безпеки стратегічно важливих об'єктів та систем. Правові механізми охоплюють питання взаємодії суб'єктів сектору безпеки і оборони з операторами критичної інфраструктури, порядок реагування на кіберінциденти та проведення спільних навчань. Нормативно-правова база передбачає створення галузевих центрів реагування на кіберінциденти та механізмів обміну інформацією про кіберзагрози [28, 33].

Правове регулювання міжвідомчої взаємодії силових структур спрямоване на забезпечення координації дій та ефективного обміну інформацією під час виконання завдань із забезпечення кібербезпеки. Законодавство визначає механізми спільного планування та проведення операцій, порядок створення міжвідомчих робочих груп та координаційних органів. Нормативно-правова база охоплює питання розмежування повноважень та відповідальності між суб'єктами сектору безпеки і оборони у сфері кібербезпеки [47, 48].

Законодавче забезпечення міжнародного співробітництва силових структур у сфері кібербезпеки створює правову основу для участі підрозділів сектору безпеки і оборони у міжнародних операціях та навчаннях. Правові механізми регулюють порядок обміну інформацією з іноземними партнерами, проведення спільних розслідувань та надання взаємної правової допомоги у справах про кіберзлочини. Нормативна база передбачає можливість створення спільних центрів реагування на кіберзагрози та механізмів оперативного обміну інформацією.

Конституційно-правові засади забезпечення кібербезпеки України реалізуються через комплексну систему нормативно-правового регулювання, котра охоплює фундаментальні положення Основного Закону держави та

спеціалізоване законодавство у сфері кібербезпеки. Нормативно-правове підґрунтя функціонування національної системи кібербезпеки формується з урахуванням динамічного характеру загроз та викликів у кіберпросторі, необхідності створення ефективних механізмів протидії кіберзлочинності та забезпечення захисту критичної інформаційної інфраструктури [15]. Стратегічні документи державної політики у сфері кібербезпеки визначають довгострокові пріоритети та напрями розвитку системи кіберзахисту держави. Законодавче регулювання охоплює широкий спектр питань, пов'язаних із забезпеченням безпеки інформаційних ресурсів, захистом персональних даних, протидією кібертероризму та іншим протиправним діям у кіберпросторі [28]. Правові механізми державно-приватного партнерства створюють підґрунтя для ефективної взаємодії державного та приватного секторів у сфері кібербезпеки, об'єднання ресурсів та можливостей усіх зацікавлених сторін.

Законодавче забезпечення діяльності силових структур у кіберпросторі базується на системному підході до визначення компетенції та повноважень суб'єктів сектору безпеки і оборони [44]. Нормативно-правова база охоплює питання організації оперативно-розшукової, контррозвідувальної та розвідувальної діяльності, проведення спеціальних операцій та заходів із протидії кіберзагрозам. Правове регулювання діяльності підрозділів кіберполіції спрямоване на забезпечення ефективного розслідування кримінальних правопорушень, вчинених з використанням інформаційних технологій. Механізми правового забезпечення кібероборони держави передбачають чітке визначення повноважень військових формувань та спеціальних служб щодо захисту суверенітету у кіберпросторі [52]. Законодавство встановлює порядок застосування сил та засобів сектору безпеки і оборони для протидії кібератакам, порядок функціонування системи ситуаційних центрів та спеціалізованих підрозділів. Нормативно-правове регулювання розвідувальної діяльності у кіберпросторі враховує необхідність

протидії розвідувально-підривній діяльності та забезпечення інформаційної переваги в умовах гібридних загроз [31].

Правове регулювання захисту критичної інформаційної інфраструктури визначає механізми взаємодії суб'єктів сектору безпеки і оборони з операторами критичної інфраструктури, порядок реагування на кіберінциденти та проведення спільних навчань. Законодавча база передбачає створення галузевих центрів реагування на кіберінциденти та механізмів обміну інформацією про кіберзагрози між усіма залученими суб'єктами.

Міжвідомча взаємодія силових структур у сфері кібербезпеки регулюється комплексом нормативно-правових актів, які визначають механізми спільного планування та проведення операцій, порядок створення координаційних органів та робочих груп [60]. Правові механізми міжнародного співробітництва створюють підґрунтя для участі підрозділів сектору безпеки і оборони у міжнародних операціях, проведення спільних розслідувань та обміну інформацією з іноземними партнерами. Законодавче регулювання підготовки фахівців з кібербезпеки та проведення наукових досліджень спрямоване на розвиток кадрового та наукового потенціалу національної системи кібербезпеки [17]. Правові механізми стимулювання розвитку індустрії кібербезпеки створюють умови для впровадження інноваційних технологій та рішень у сфері кіберзахисту. Міжнародно-правове співробітництво у сфері кібербезпеки базується на міжнародних договорах та угодах, які визначають форми та механізми взаємодії з іноземними партнерами.

Висновки до розділу 2

1. Нормативно-правова база у сфері кібербезпеки України демонструє поступовий розвиток від фрагментарного регулювання окремих питань до формування цілісної системи правових норм, хоча все ще потребує гармонізації з міжнародними стандартами та адаптації до сучасних викликів гібридної війни.

РОЗДІЛ 3
АНАЛІЗ ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР УКРАЇНИ ЩОДО ЗАХИСТУ КІБЕРПРОСТОРУ

3.1. Система забезпечення кібербезпеки України: структура та повноваження основних суб'єктів

Рада національної безпеки і оборони України виступає центральним координаційним органом у системі забезпечення кібернетичної безпеки держави. Повноваження РНБО в контексті кіберзахисту держави визначаються положеннями Конституції України, Закону України «Про національну безпеку України» та Стратегії кібербезпеки України. Фундаментальною функцією РНБО постає координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки в кіберпросторі. Система забезпечення кібербезпеки України під керівництвом РНБО реалізує комплексний підхід до протидії кіберзагрозам через впровадження організаційно-технічних моделей кіберзахисту. Стратегічне планування та прогнозування у сфері кібербезпеки здійснюється через механізми координації діяльності суб'єктів сектору безпеки та оборони України. РНБО формує систему ситуаційних центрів державних органів сектору безпеки й оборони та забезпечує функціонування національної системи виявлення та реагування на кіберінциденти.

Національний координаційний центр кібербезпеки як робочий орган РНБО України забезпечує координацію діяльності суб'єктів сектору безпеки та оборони України під час реалізації Стратегії кібербезпеки України. НКЦК здійснює аналіз стану кібербезпеки, формує пропозиції щодо забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформаційно-телекомунікаційних систем, об'єктів критичної інформаційної інфраструктури.

Таблиця 2.1

Основні суб'єкти національної системи кібербезпеки України

Суб'єкт	Ключові функції у сфері кібербезпеки	Нормативно-правова основа діяльності
РНБО України	Координація та контроль діяльності суб'єктів сектору безпеки і оборони	Закон України «Про національну безпеку України»
Національний координаційний центр кібербезпеки	Координація та контроль діяльності у сфері кібербезпеки	Указ Президента України №242/2016
Держспецзв'язку	Формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації	Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»
СБУ	Контррозвідувальний та оперативно-розшуковий захист кіберпростору	Закон України «Про Службу безпеки України»
Кіберполіція	Протидія кіберзлочинності та забезпечення кібербезпеки	Положення про Департамент кіберполіції Національної поліції України

Джерело: *складено автором на основі [14]*

Повноваження РНБО охоплюють координацію заходів кібероборони в рамках протидії збройній агресії, участь у формуванні міжнародної коаліції для протистояння кіберзагрозам, налагодження механізмів обміну інформацією з міжнародними партнерами. РНБО координує розробку індикаторів кіберзагроз, методик протидії та програм підвищення цифрової грамотності населення. Система забезпечення кібербезпеки під егідою РНБО функціонує через механізми міжвідомчої взаємодії та створення спільних робочих груп для виконання завдань кіберзахисту. Аналітична складова роботи РНБО реалізується через моніторинг кіберпростору, виявлення та оцінку потенційних загроз національній безпеці України в кіберсфері. РНБО координує проведення навчань з питань кібербезпеки та кібероборони для відпрацювання взаємодії між суб'єктами забезпечення кібербезпеки. Організація таких навчань дозволяє перевірити готовність національної системи кібербезпеки до відбиття масштабних кібератак та удосконалити механізми реагування на кіберінциденти.

Масштабна цифровізація державного управління та розвиток електронних послуг зумовлюють розширення повноважень РНБО у сфері захисту національного кіберпростору. РНБО координує впровадження технологій кіберзахисту в роботу органів державної влади, формування системи аудиту інформаційної безпеки та проведення оцінки захищеності державних інформаційних ресурсів. Модернізація системи кібербезпеки України під керівництвом РНБО передбачає впровадження новітніх технологій, зокрема систем виявлення вторгнень, засобів криптографічного захисту інформації, створення галузевих центрів реагування на кіберінциденти. Розвиток державно-приватного партнерства у сфері кібербезпеки реалізується через механізми обміну інформацією про кіберзагрози та спільну протидію кібератакам. Законодавча база функціонування системи кібербезпеки України постійно вдосконалюється з урахуванням нових викликів та загроз. РНБО бере активну участь у формуванні нормативно-правового забезпечення кібербезпеки через підготовку проектів законів, указів Президента України, рішень РНБО України з питань забезпечення кібербезпеки держави. Міжнародне співробітництво у сфері кібербезпеки координується РНБО через механізми обміну інформацією з партнерськими безпековими структурами, участь у міжнародних навчаннях, розробку спільних методик протидії кіберзагрозам. Розвиток потенціалу України у сфері кібербезпеки передбачає інтеграцію національної системи кіберзахисту до відповідних європейських та євроатлантичних безпекових механізмів.

Державна служба спеціального зв'язку та захисту інформації України функціонує як центральний орган виконавчої влади зі спеціальним статусом, забезпечуючи формування та реалізацію державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України. Нормативно-правовою основою діяльності Держспецзв'язку виступають Закони України «Про Державну службу спеціального зв'язку та захисту

інформації України», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах».

Формування та реалізація державної політики у сфері захисту державних інформаційних ресурсів здійснюється Держспецзв'язку через впровадження комплексних систем захисту інформації, проведення державної експертизи у сфері криптографічного та технічного захисту інформації. Служба забезпечує функціонування Державного центру кіберзахисту, який здійснює моніторинг стану захищеності державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Оперативно-технічні підрозділи Держспецзв'язку забезпечують безперебійне функціонування Національної системи конфіденційного зв'язку, яка використовується для обміну інформацією з обмеженим доступом між органами державної влади. Система захищеного урядового зв'язку дозволяє здійснювати обмін службовою інформацією між посадовими особами в умовах підвищених загроз національній безпеці. Підрозділи технічного захисту інформації Держспецзв'язку здійснюють контроль за дотриманням вимог нормативних документів з технічного захисту інформації, проводять оцінку захищеності об'єктів інформаційної діяльності та інформаційно-телекомунікаційних систем. Розробка та впровадження новітніх технологій захисту інформації реалізується через діяльність науково-дослідних установ, які входять до сфери управління Держспецзв'язку.

Сертифікація засобів технічного та криптографічного захисту інформації становить вагомий напрям діяльності Держспецзв'язку. Служба здійснює державний контроль за якістю послуг, які надаються операторами та провайдерами телекомунікацій, забезпечує проведення випробувань комплексних систем захисту інформації. Модернізація національної системи технічного та криптографічного захисту інформації відбувається через впровадження сучасних методів криптографічного перетворення інформації, розробку та застосування національних криптографічних алгоритмів.

Держспецзв'язку координує роботи з проектування, впровадження та експлуатації комплексних систем захисту інформації в державних органах.

Міжнародна співпраця Держспецзв'язку реалізується через участь у міжнародних організаціях з питань інформаційної безпеки, обмін досвідом із партнерськими службами іноземних держав, гармонізацію національних стандартів у сфері криптографічного та технічного захисту інформації з міжнародними стандартами. Служба бере активну участь у реалізації міжнародних проектів технічної допомоги у сфері кібербезпеки. Система підготовки та підвищення кваліфікації фахівців з кібербезпеки розвивається через діяльність відомчих навчальних закладів Держспецзв'язку. Підготовка кадрів здійснюється за спеціальностями кібербезпеки, телекомунікацій, захисту інформації та управління інформаційною безпекою. Практична підготовка фахівців реалізується через залучення до реальних проектів із впровадження систем захисту інформації.

Державний центр кіберзахисту Держспецзв'язку забезпечує функціонування команди реагування на комп'ютерні надзвичайні події CERT-UA, яка здійснює моніторинг кіберзагроз, накопичення та аналіз даних про кіберінциденти, розробку рекомендацій щодо протидії кіберзагрозам. CERT-UA координує обмін інформацією про кіберінциденти з міжнародними партнерами, надає консультативну допомогу об'єктам критичної інформаційної інфраструктури. Забезпечення сталого функціонування національної системи захищеного доступу державних органів до мережі Інтернет реалізується через впровадження комплексних систем захисту інформації, проведення моніторингу стану захищеності інформаційно-телекомунікаційних систем, протидію кібератакам на державні інформаційні ресурси. Держспецзв'язку координує заходи з підвищення рівня захищеності державних електронних інформаційних ресурсів від несанкціонованого доступу. Кіберпідрозділи Служби безпеки України становлять потужну складову системи забезпечення кібербезпеки держави, реалізуючи комплекс контррозвідувальних та оперативно-розшукових заходів у кіберпросторі.

Структурні підрозділи СБУ, відповідальні за кібербезпеку, функціонують на основі Закону України «Про Службу безпеки України» та Стратегії кібербезпеки України, забезпечуючи захист державного суверенітету та конституційного ладу від протиправних посягань з використанням кіберпростору.

Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ здійснює моніторинг кіберпростору з метою виявлення, попередження та припинення розвідувально-підривної діяльності іноземних спецслужб. Підрозділи кібербезпеки СБУ проводять комплексні заходи з протидії кібершпигунству, виявлення та блокування діяльності кібертерористичних угруповань, запобігання спробам дестабілізації суспільно-політичної ситуації через кіберпростір. Оперативно-технічні підрозділи СБУ забезпечують проведення спеціальних технічних заходів у кіберпросторі, спрямованих на виявлення та документування протиправної діяльності. Розробка та впровадження новітніх технічних рішень для протидії кіберзагрозам реалізується через взаємодію з науково-дослідними установами та провідними ІТ-компаніями України.

Міжнародна співпраця кіберпідрозділів СБУ охоплює обмін інформацією про кіберзагрози з партнерськими спецслужбами, проведення спільних операцій з виявлення та припинення діяльності транснаціональних хакерських угруповань. Налагоджено механізми оперативного обміну технічними індикаторами кібератак та методиками протидії новітнім кіберзагрозам з відповідними підрозділами спецслужб країн-партнерів. Система підготовки фахівців з кібербезпеки для підрозділів СБУ базується на поєднанні теоретичної підготовки та практичного досвіду протидії реальним кіберзагрозам. Навчальні програми охоплюють питання проведення комп'ютерно-технічних експертиз, методики виявлення та документування кіберзлочинів, особливості проведення спеціальних технічних заходів у кіберпросторі. Аналітичні підрозділи СБУ здійснюють моніторинг та оцінку загроз національній безпеці у кіберпросторі, формують прогнози розвитку

ситуації та розробляють рекомендації щодо протидії виявленим загрозам. Аналітична робота передбачає використання сучасних систем збору та обробки інформації, застосування методів прогнозного моделювання та сценарного аналізу розвитку кіберзагроз.

Ситуаційні центри кібербезпеки СБУ забезпечують координацію дій підрозділів служби під час виявлення та реагування на кіберінциденти, проведення спеціальних операцій у кіберпросторі. Функціонування ситуаційних центрів базується на використанні автоматизованих систем управління та підтримки прийняття рішень, що дозволяє оперативно реагувати на зміни кібербезпекової ситуації.

Протидія інформаційно-психологічним операціям противника у кіберпросторі реалізується через виявлення та блокування діяльності мереж ботів, виявлення та документування фактів поширення дезінформації через соціальні мережі та месенджери. Кіберпідрозділи СБУ здійснюють моніторинг соціальних мереж та медіапростору для виявлення спроб маніпулювання суспільною свідомістю та координації протестних акцій через кіберпростір. Забезпечення безпеки об'єктів критичної інформаційної інфраструктури реалізується кіберпідрозділами СБУ через проведення аудитів інформаційної безпеки, надання рекомендацій щодо посилення систем захисту, координацію заходів з протидії кібератакам. Служба забезпечує оперативне реагування на спроби несанкціонованого втручання в роботу систем управління об'єктами критичної інфраструктури.

Науково-технічний потенціал кіберпідрозділів СБУ розвивається через взаємодію з провідними науковими установами, участь у розробці та впровадженні інноваційних технологій кіберзахисту. Служба бере активну участь у формуванні національної системи підготовки фахівців з кібербезпеки, розвитку науково-технічної бази для проведення досліджень у сфері інформаційної безпеки.

Національна поліція України через Департамент кіберполіції реалізує комплексну державну політику у сфері протидії кіберзлочинності та

забезпечення кібербезпеки. Структурні підрозділи кіберполіції функціонують на основі Закону України «Про Національну поліцію» та Положення про Департамент кіберполіції, здійснюючи оперативно-розшукову діяльність та досудове розслідування кіберзлочинів. Підрозділи кіберполіції забезпечують реалізацію програм протидії кіберзлочинності через проведення спеціальних операцій з виявлення та документування злочинів, скоєних з використанням високих інформаційних технологій. Оперативні підрозділи здійснюють моніторинг кіберпростору для виявлення фактів несанкціонованого втручання в роботу комп'ютерних систем, розповсюдження шкідливого програмного забезпечення, онлайн-шахрайства та інших протиправних дій. Розслідування кіберзлочинів здійснюється слідчими підрозділами Національної поліції із залученням профільних фахівців Департаменту кіберполіції. Методика розслідування охоплює проведення комп'ютерно-технічних експертиз, аналіз цифрових доказів, встановлення причинно-наслідкових зв'язків між діями зловмисників та наслідками кібератак. Експертно-криміналістичні підрозділи забезпечують технічний супровід розслідування через проведення експертних досліджень комп'ютерної техніки та програмного забезпечення. Міжнародна співпраця Департаменту кіберполіції реалізується через участь у спільних операціях з правоохоронними органами інших держав, обмін інформацією про кіберзлочини через канали Інтерполу та Європолу. Налагоджено механізми оперативного обміну інформацією про нові види кіберзагроз, методи вчинення кіберзлочинів та способи протидії кіберзлочинності з правоохоронними органами країн-партнерів.

Превентивна діяльність підрозділів кіберполіції спрямована на підвищення обізнаності населення щодо кіберзагроз, проведення просвітницьких заходів з питань кібергігієни, надання рекомендацій щодо захисту персональних даних та безпечного користування інтернет-сервісами. Департамент кіберполіції регулярно проводить інформаційні кампанії з попередження онлайн-шахрайства, протидії кібербулінгу та захисту дітей в інтернеті. Аналітичні підрозділи Департаменту кіберполіції здійснюють збір

та аналіз інформації про тенденції розвитку кіберзлочинності, формують прогнози появи нових видів кіберзагроз, розробляють методичні рекомендації щодо виявлення та документування кіберзлочинів. Застосування сучасних аналітичних інструментів дозволяє виявляти закономірності у діяльності організованих злочинних угруповань, які спеціалізуються на скоєнні кіберзлочинів.

Регіональні підрозділи кіберполіції забезпечують оперативне реагування на повідомлення про кіберінциденти, проведення першочергових слідчих дій на місцях скоєння кіберзлочинів, взаємодію з територіальними підрозділами інших правоохоронних органів. Система підготовки особового складу передбачає регулярне підвищення кваліфікації працівників кіберполіції, освоєння нових методів виявлення та документування кіберзлочинів. Протидія шахрайським схемам в інтернеті реалізується через моніторинг підозрілої активності на торговельних майданчиках, виявлення фішингових сайтів, блокування шахрайських телефонних номерів та банківських рахунків. Департамент кіберполіції активно взаємодіє з банківськими установами та платіжними системами для попередження фінансових злочинів у кіберпросторі.

Науково-технічне забезпечення діяльності підрозділів кіберполіції охоплює впровадження сучасних технічних засобів для проведення комп'ютерно-технічних експертиз, розробку спеціалізованого програмного забезпечення для аналізу цифрових доказів, створення автоматизованих систем моніторингу кіберпростору. Модернізація технічної бази здійснюється з урахуванням світових тенденцій розвитку технологій протидії кіберзлочинності. Взаємодія з громадськістю та бізнес-середовищем реалізується через функціонування контактного центру кіберполіції, проведення спільних навчань та тренінгів, обмін інформацією про актуальні кіберзагрози. Налагоджено механізми оперативного інформування про виявлені вразливості в інформаційних системах, надання технічних консультацій щодо захисту від кібератак. Координація діяльності силових

структур у кіберпросторі реалізується через багаторівневу систему міжвідомчої взаємодії під загальним керівництвом Ради національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган РНБО забезпечує узгодження дій суб'єктів сектору безпеки та оборони під час реалізації Стратегії кібербезпеки України.

Механізми міжвідомчої координації охоплюють створення спільних робочих груп для виконання завдань кіберзахисту, проведення міжвідомчих навчань з питань кібербезпеки, формування єдиних методологічних підходів до організації кіберзахисту державних інформаційних ресурсів. Спільні оперативні штаби забезпечують координацію дій силових структур під час виявлення та реагування на масштабні кібератаки, проведення спеціальних операцій у кіберпросторі. Обмін інформацією між силовими структурами здійснюється через захищені канали урядового зв'язку, спеціалізовані системи обміну даними про кіберінциденти, платформи оперативної взаємодії підрозділів кібербезпеки. Служба безпеки України, Держспецзв'язку, кіберполіція та інші суб'єкти забезпечення кібербезпеки налагодили систему оперативного інформування про виявлені кіберзагрози та вжиті заходи реагування.

Спільні навчання підрозділів кібербезпеки різних відомств проводяться регулярно для відпрацювання алгоритмів реагування на кризові ситуації, перевірки готовності систем захисту критичної інфраструктури, вдосконалення механізмів координації дій під час масштабних кібератак. Сценарії навчань розробляються з урахуванням актуальних кіберзагроз та прогнозованих напрямків розвитку кіберзлочинності. Аналітична складова міжвідомчої взаємодії реалізується через спільну оцінку кіберзагроз, розробку прогнозів розвитку ситуації у кіберпросторі, формування єдиних підходів до категоризації та оцінки наслідків кіберінцидентів. Аналітичні підрозділи силових структур здійснюють обмін результатами моніторингу кіберпростору, узагальнюють інформацію про нові види кіберзагроз та методи протидії. Координація міжнародного співробітництва силових структур у

сфері кібербезпеки здійснюється через механізми взаємодії з партнерськими безпековими структурами інших держав, участь у міжнародних навчаннях та тренінгах, обмін досвідом протидії кіберзагрозам. Налагоджено механізми оперативного обміну інформацією про транскордонні кіберінциденти з правоохоронними органами країн-партнерів.

Науково-технічна співпраця підрозділів кібербезпеки різних відомств реалізується через спільну розробку та впровадження технічних рішень для протидії кіберзагрозам, створення єдиних баз даних про кіберінциденти, розробку методик проведення комп'ютерно-технічних експертиз. Відомчі науково-дослідні установи координують роботу з розробки та впровадження інноваційних технологій кіберзахисту. Система підготовки кадрів для підрозділів кібербезпеки силових структур базується на єдиних стандартах професійної підготовки, узгоджених навчальних програмах, спільному використанні навчально-матеріальної бази відомчих навчальних закладів. Міжвідомчі програми підвищення кваліфікації забезпечують формування єдиних підходів до організації кіберзахисту.

Координація заходів з протидії інформаційно-психологічним операціям противника реалізується через спільний моніторинг інформаційного простору, виявлення та блокування каналів поширення дезінформації, проведення узгоджених інформаційних кампаній. Силові структури забезпечують комплексну протидію спробам маніпулювання суспільною свідомістю через кіберпростір. Модернізація системи міжвідомчої координації передбачає впровадження автоматизованих систем управління та підтримки прийняття рішень, створення єдиної системи ситуаційних центрів кібербезпеки, розвиток захищеної інфраструктури обміну інформацією між суб'єктами забезпечення кібербезпеки. Удосконалення нормативно-правової бази міжвідомчої взаємодії здійснюється з урахуванням практичного досвіду протидії кіберзагрозам.

3.2. Основні напрями діяльності силових структур у сфері кіберзахисту

Запобігання та протидія кібератакам становлять комплексний напрям діяльності силових структур України, спрямований на захист національного кіберпростору від деструктивного впливу. Система протидії кібератакам базується на багаторівневому підході до забезпечення кібербезпеки та координації зусиль різних державних органів. Державний центр кіберзахисту впроваджує проактивні заходи захисту державних інформаційних ресурсів через розгортання систем виявлення та запобігання вторгненням, проведення регулярного тестування на проникнення, оцінку вразливостей інформаційних систем. Технології захисту від DDoS-атак забезпечують безперервність функціонування критичних інформаційних сервісів державних органів.

Оперативні підрозділи СБУ здійснюють заходи з виявлення та припинення розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Контррозвідувальні операції спрямовані на викриття та документування діяльності кібершпигунських мереж, блокування спроб несанкціонованого доступу до державних інформаційних ресурсів з боку іноземних технічних розвідок. Технології активного кіберзахисту впроваджуються через створення систем-пасток для зловмисників, проведення превентивних кібероперацій, блокування командних центрів керування шкідливим програмним забезпеченням. Використання методів дезінформації та відволікання уваги зловмисників дозволяє знижувати ефективність спланованих кібератак.

Підрозділи кіберполіції забезпечують оперативне реагування на масові фішингові розсилки, блокування шахрайських веб-ресурсів, протидію розповсюдженню шкідливого програмного забезпечення. Взаємодія з банківськими установами та платіжними системами дозволяє оперативно блокувати рахунки кіберзлочинців та запобігати легалізації злочинних доходів.

Таблиця 2.2

Класифікація основних типів кібератак та методів протидії

Тип кібератаки	Характеристика атаки	Методи протидії	Відповідальні підрозділи
DDoS-атаки	Розподілені атаки на відмову в обслуговуванні	Фільтрація трафіку, розподіл навантаження, захист периметра	Держспецзв'язку, CERT-UA
APT-атаки	Цільові довготривалі атаки з використанням складних методів	Багаторівневий захист, поведінковий аналіз, сегментація мереж	СБУ, розвідувальні органи
Фішинг	Викрадення облікових даних через підроблені ресурси	Моніторинг доменів, блокування фішингових сайтів	Кіберполіція, CERT-UA
Програми-вимагачі	Шифрування даних з вимогою викупу	Резервне копіювання, оновлення систем	Держспецзв'язку, Кіберполіція
Соціальна інженерія	Маніпулювання користувачами для отримання доступу	Навчання персоналу, контроль доступу	Міжвідомчі робочі групи

Джерело: *складено автором на основі [51]*

Система захисту від програм-вимагачів базується на впровадженні комплексних рішень резервного копіювання даних, сегментації мереж, контролю доступу до критичних систем. Розроблені методики аварійного відновлення систем після кібератак дозволяють мінімізувати наслідки застосування шкідливого програмного забезпечення. Протидія соціальній інженерії реалізується через проведення навчань персоналу, впровадження політик інформаційної безпеки, контроль за дотриманням правил поводження з конфіденційною інформацією. Програми підвищення обізнаності користувачів охоплюють питання виявлення фішингових атак, протидії методам соціальної інженерії, захисту облікових даних.

Міжвідомча взаємодія у сфері протидії кібератакам забезпечується через функціонування спільних оперативних штабів, проведення спеціальних операцій, обмін інформацією про нові методи кібератак. Координація дій різних підрозділів дозволяє забезпечити комплексний підхід до нейтралізації кіберзагроз. Інструменти криміналістичного аналізу кібератак використовуються для встановлення методів проникнення в системи, дослідження механізмів поширення шкідливого програмного забезпечення,

виявлення слідів діяльності зловмисників. Результати аналізу використовуються для вдосконалення систем захисту та розробки нових методів протидії кібератакам.

Розслідування кіберзлочинів становить складний комплекс слідчих дій та оперативно-розшукових заходів, спрямованих на встановлення всіх обставин протиправних діянь у кіберпросторі. Методологія розслідування кіберзлочинів базується на поєднанні класичних криміналістичних методів та спеціалізованих технік комп'ютерно-технічної експертизи. Підрозділи кіберполіції здійснюють досудове розслідування кримінальних правопорушень через проведення невідкладних слідчих дій, спрямованих на фіксацію цифрових доказів, встановлення обставин скоєння злочину, виявлення причетних осіб. Слідчі-криміналісти використовують спеціалізоване програмне забезпечення для збору та аналізу цифрових слідів, відновлення видалених даних, дослідження шкідливого програмного забезпечення. Експертно-криміналістичні підрозділи проводять комплексні дослідження комп'ютерної техніки, мобільних пристроїв, носіїв інформації для отримання доказової бази. Методики комп'ютерно-технічної експертизи охоплюють аналіз файлових систем, дослідження мережевого трафіку, відновлення історії дій користувачів, аналіз метаданих файлів. Сучасні криміналістичні лабораторії оснащені спеціалізованим обладнанням для проведення експертних досліджень у сфері кіберзлочинності.

Аналітичне супроводження розслідування забезпечується через використання систем кримінального аналізу, побудову схем зв'язків між фігурантами кримінальних проваджень, аналіз фінансових транзакцій, пов'язаних з кіберзлочинами. Методи великих даних застосовуються для виявлення прихованих закономірностей у діяльності організованих злочинних угруповань, які спеціалізуються на кіберзлочинах. Міжнародна правова допомога у розслідуванні кіберзлочинів реалізується через механізми співпраці з правоохоронними органами інших держав, обмін доказовою інформацією, проведення спільних слідчих дій. Процедури збору цифрових

доказів уніфіковані відповідно до міжнародних стандартів для забезпечення можливості використання зібраних матеріалів у судах різних юрисдикцій. Оперативно-розшукові заходи спрямовані на встановлення місцезнаходження підозрюваних, документування фактів протиправної діяльності, виявлення каналів легалізації злочинних доходів. Підрозділи кіберполіції використовують методи оперативного впровадження в злочинні угруповання для отримання інформації про плановані кіберзлочини та механізми їх вчинення.

Методика розслідування шахрайств у сфері електронної комерції передбачає аналіз транзакцій платіжних систем, встановлення реальних бенефіціарів шахрайських операцій, блокування рахунків злочинців. Взаємодія з банківськими установами дозволяє отримувати інформацію про рух коштів, пов'язаних з кіберзлочинами, та вживати заходів щодо їх повернення потерпілим. Розслідування кібершпигунства здійснюється контррозвідувальними підрозділами СБУ через проведення комплексу оперативно-технічних заходів, спрямованих на встановлення джерел витоку інформації, виявлення каналів передачі розвідувальних даних, документування діяльності агентурних мереж іноземних спецслужб у кіберпросторі.

Криміналістичне дослідження шкідливого програмного забезпечення проводиться в спеціалізованих лабораторіях з використанням методів зворотної інженерії, аналізу поведінки програм у тестовому середовищі, дослідження механізмів поширення та управління шкідливим кодом. Результати досліджень використовуються для розробки методів протидії новим видам кіберзагроз. Підготовка доказової бази для судового розгляду справ про кіберзлочини вимагає дотримання процесуальних вимог щодо збору та фіксації цифрових доказів, забезпечення належного документування слідчих дій, проведення експертних досліджень. Формування матеріалів кримінальних проваджень здійснюється з урахуванням специфіки доказування у справах про кіберзлочини. Профілактична складова

розслідування кіберзлочинів реалізується через аналіз способів вчинення злочинів, виявлення вразливостей інформаційних систем, які використовувались злочинцями, розробку рекомендацій щодо посилення захисту від подібних злочинів у майбутньому. Узагальнення слідчої практики дозволяє вдосконалювати методики розслідування та попередження кіберзлочинів.

Таблиця 2.3

Система захисту об'єктів критичної інформаційної інфраструктури

Рівень захисту	**Заходи безпеки**	**Технічні засоби**	**Відповідальні органи**
Організаційний	Політики безпеки, регламенти доступу, навчання персоналу	Системи контролю доступу, відеоспостереження	Держспецзв'язку, служби безпеки об'єктів
Мережевий	Сегментація мереж, фільтрація трафіку	Міжмережеві екрани, системи виявлення вторгнень	CERT-UA, технічні підрозділи
Прикладний	Захист додатків, шифрування даних	Антивірусні системи, засоби криптографічного захисту	Підрозділи кібербезпеки
Фізичний	Контроль периметру, охорона об'єктів	Системи фізичного захисту, датчики	Служби охорони, СБУ
Моніторинг	Контроль подій безпеки, аудит систем	Системи моніторингу, SIEM-системи	Ситуаційні центри, SOC

Джерело: *складено автором на основі [32]*

Захист критичної інформаційної інфраструктури становить пріоритетний напрям діяльності силових структур у сфері забезпечення кібербезпеки держави. Комплексна система захисту об'єктів критичної інфраструктури базується на багаторівневому підході до забезпечення безпеки інформаційних систем та мереж. Держспецзв'язку здійснює координацію заходів із захисту критичної інформаційної інфраструктури через впровадження уніфікованих вимог до систем захисту, проведення аудитів інформаційної безпеки, надання методичної допомоги операторам критичної інфраструктури. Система державного контролю охоплює моніторинг стану захищеності об'єктів, оцінку

ефективності впроваджених заходів безпеки, перевірку готовності до реагування на кіберінциденти.

Технології захисту критичної інформаційної інфраструктури передбачають впровадження систем виявлення та запобігання вторгненням, засобів криптографічного захисту інформації, механізмів контролю доступу до критичних систем. Архітектура безпеки будується за принципом глибокоешелонованої оборони з використанням різних технологічних рішень на кожному рівні захисту.

Підрозділи кібербезпеки СБУ забезпечують контррозвідувальний захист об'єктів критичної інфраструктури через проведення оперативно-технічних заходів з виявлення та припинення розвідувально-підривної діяльності. Оперативне супроводження об'єктів дозволяє своєчасно виявляти загрози та вживати заходів щодо їх нейтралізації. Системи моніторингу безпеки критичної інфраструктури функціонують у режимі реального часу, забезпечуючи збір та аналіз інформації про події безпеки, виявлення аномальної активності, формування сигналів тривоги при виявленні ознак кібератак. Ситуаційні центри кібербезпеки здійснюють цілодобовий моніторинг стану захищеності об'єктів та координацію дій з реагування на інциденти.

Методика оцінки загроз для об'єктів критичної інфраструктури базується на аналізі вразливостей систем, моделюванні можливих сценаріїв атак, оцінці потенційних наслідків. Результати оцінки використовуються для пріоритезації заходів захисту та розподілу ресурсів на забезпечення кібербезпеки. Плани забезпечення безперервності функціонування критичної інфраструктури передбачають створення резервних систем управління, впровадження механізмів аварійного відновлення, регулярне проведення навчань з відпрацювання дій у кризових ситуаціях. Розроблені процедури реагування на різні типи кіберінцидентів, включаючи повне відключення автоматизованих систем управління. Міжнародна співпраця у сфері захисту критичної інфраструктури реалізується через обмін інформацією про загрози,

проведення спільних навчань, гармонізацію підходів до забезпечення кібербезпеки. Налагоджено механізми оперативного інформування партнерських структур про виявлені загрози глобального характеру.

Науково-технічний супровід захисту критичної інфраструктури здійснюється через розробку нових технологій кіберзахисту, проведення досліджень у сфері промислової кібербезпеки, створення спеціалізованих засобів захисту автоматизованих систем управління технологічними процесами. Впровадження інноваційних рішень дозволяє підвищувати рівень захищеності об'єктів від сучасних кіберзагроз. Підготовка фахівців з захисту критичної інфраструктури реалізується через спеціалізовані навчальні програми, які охоплюють питання безпеки промислових систем управління, захисту технологічних мереж, реагування на інциденти безпеки. Практична підготовка здійснюється на спеціалізованих полігонах з використанням реального обладнання та систем управління.

3.3. Взаємодія силових структур України у протидії кіберзагрозам в умовах війни

В умовах повномасштабної війни механізми координації дій силових структур України у кіберпросторі набули особливого значення та зазнали суттєвої трансформації. Національний координаційний центр кібербезпеки при РНБО України виступає центральним елементом системи міжвідомчої взаємодії, забезпечуючи узгодження заходів протидії кіберзагрозам воєнного характеру. Спільні оперативні штаби з питань кібербезпеки функціонують у цілодобовому режимі, забезпечуючи координацію дій різних відомств при виявленні та нейтралізації кібератак противника. Представники СБУ, Держспецзв'язку, кіберполіції та інших силових структур здійснюють оперативний обмін інформацією про виявлені загрози та координують заходи реагування на кіберінциденти воєнного характеру.

Система ситуаційних центрів кібербезпеки силових структур об'єднана в єдину мережу, що забезпечує формування комплексної картини кіберзагроз у масштабах держави. Автоматизовані системи управління та підтримки прийняття рішень дозволяють оперативно розподіляти завдання між різними підрозділами та координувати спільні дії з протидії кібератакам противника. Механізми координації охоплюють створення міжвідомчих робочих груп для виконання спеціальних завдань у кіберпросторі, проведення спільних навчань та тренувань, розробку єдиних методик протидії новітнім видам кіберзагроз. Налагоджено систему постійних консультацій між керівництвом підрозділів кібербезпеки різних відомств для узгодження стратегічних питань забезпечення кібероборони держави. Координація дій з територіальними підрозділами силових структур здійснюється через регіональні координаційні центри кібербезпеки, які забезпечують оперативне реагування на кіберінциденти на місцевому рівні. Розгорнута мережа мобільних груп реагування на кіберінциденти дозволяє оперативно надавати допомогу об'єктам критичної інфраструктури при виявленні ознак кібератак.

Система обміну інформацією про кіберзагрози між силовими структурами базується на використанні захищених каналів зв'язку та спеціалізованих платформ обміну даними про кіберінциденти. Впроваджені автоматизовані системи збору та аналізу інформації про кібератаки забезпечують формування єдиної бази даних про тактику та методи дій противника у кіберпросторі. Спільні операції силових структур у кіберпросторі проводяться на основі розроблених планів взаємодії та передбачають чіткий розподіл завдань між різними підрозділами. Контррозвідувальні підрозділи СБУ забезпечують виявлення та документування розвідувально-підривної діяльності противника, підрозділи Держспецзв'язку здійснюють технічні заходи з блокування кібератак, кіберполіція проводить розслідування виявлених кіберзлочинів. Міжвідомчі групи швидкого реагування на кіберінциденти забезпечують оперативне реагування на масштабні кібератаки противника, проведення першочергових

заходів з локалізації наслідків атак, відновлення працездатності уражених систем. Налагоджено механізми залучення експертів різних відомств для проведення спільних розслідувань складних кіберінцидентів.

Аналітична підтримка спільних операцій реалізується через створення міжвідомчих аналітичних груп, які здійснюють комплексний аналіз кіберзагроз, розробку сценаріїв протидії, оцінку ефективності вжитих заходів. Результати аналітичної роботи використовуються для коригування планів спільних дій та вдосконалення механізмів міжвідомчої взаємодії. Навчання та тренування підрозділів різних відомств проводяться регулярно для відпрацювання спільних дій при різних сценаріях кібератак, перевірки ефективності механізмів координації, виявлення проблемних питань взаємодії. Сценарії навчань розробляються з урахуванням реальних прикладів кібератак противника та прогнозованих загроз. Міжнародна складова спільних операцій реалізується через взаємодію з партнерськими спецслужбами та правоохоронними органами інших держав, проведення транскордонних операцій з протидії кіберзлочинності, обмін інформацією про тактику та методи дій противника у кіберпросторі. Налагоджено механізми оперативної взаємодії з міжнародними центрами реагування на кіберінциденти.

Спільне використання технічних ресурсів та спеціального програмного забезпечення дозволяє підвищити ефективність протидії кіберзагрозам через об'єднання можливостей різних відомств. Створено єдину базу даних шкідливого програмного забезпечення, розгорнуто мережу спільних лабораторій комп'ютерно-технічних експертиз, впроваджено уніфіковані методики дослідження кіберінцидентів. Міжнародна співпраця силових структур України у сфері протидії кіберзагрозам набула особливої інтенсивності в умовах повномасштабної війни та здійснюється за багатьма напрямами взаємодії з партнерськими безпековими структурами. Координація міжнародного співробітництва реалізується через мережу офіцерів зв'язку при дипломатичних представництвах, спеціалізовані підрозділи міжнародної

взаємодії у структурі силових відомств, платформи обміну інформацією про кіберзагрози.

Служба безпеки України налагодила ефективну взаємодію з партнерськими спецслужбами країн-членів НАТО та ЄС у сфері протидії кібершпигунству та кібертероризму. Спільні операції спрямовані на виявлення та припинення діяльності хакерських угруповань, які діють в інтересах країни-агресора. Налагоджено механізми оперативного обміну розвідувальною інформацією про підготовку масштабних кібератак та методи протидії новітнім кіберзагрозам. Департамент кіберполіції Національної поліції України активно співпрацює з правоохоронними органами інших держав через канали Інтерполу та Європолу. Проведення спільних операцій дозволяє ефективно протидіяти транснаціональній кіберзлочинності, виявляти та документувати діяльність організованих злочинних угруповань у кіберпросторі. Міжнародні слідчі групи забезпечують розслідування складних кіберзлочинів, які мають транскордонний характер. Держспецзв'язку розвиває співпрацю з профільними органами країн-партнерів у сфері технічного та криптографічного захисту інформації. Гармонізація національних стандартів у сфері кібербезпеки з міжнародними вимогами дозволяє забезпечити сумісність технічних рішень та ефективну взаємодію при реагуванні на кіберінциденти. Налагоджено обмін технічними індикаторами кібератак та методиками протидії через захищені канали зв'язку. CERT-UA як національний центр реагування на кіберінциденти інтегрований у глобальну мережу команд реагування на комп'ютерні надзвичайні події. Членство у міжнародних організаціях з питань кібербезпеки забезпечує можливість оперативного обміну інформацією про кіберзагрози, участь у спільних навчаннях, доступ до міжнародних баз даних шкідливого програмного забезпечення.

Міжнародні програми технічної допомоги у сфері кібербезпеки охоплюють проекти з модернізації технічної бази підрозділів кібербезпеки, впровадження сучасних технологій захисту інформації, підготовки фахівців.

Країни-партнери надають експертну підтримку при проведенні аудитів безпеки критичної інформаційної інфраструктури, розробці методик протидії кіберзагрозам. Спільні міжнародні навчання з питань кібербезпеки проводяться регулярно для відпрацювання механізмів взаємодії при реагуванні на масштабні кібератаки. Сценарії навчань охоплюють різні типи кіберзагроз та передбачають координацію дій підрозділів кібербезпеки різних країн. Результати навчань використовуються для вдосконалення процедур міжнародної взаємодії. Науково-технічна співпраця реалізується через участь у міжнародних дослідницьких проектах, проведення спільних досліджень у сфері кібербезпеки, обмін досвідом розробки та впровадження інноваційних технологій захисту. Створено міжнародні дослідницькі лабораторії для вивчення новітніх видів кіберзагроз та розробки методів протидії. Міжнародні механізми атрибуції кібератак забезпечують можливість достовірного встановлення джерел походження кібератак та притягнення до відповідальності причетних осіб. Спільні розслідування дозволяють збирати докази причетності конкретних держав до проведення кібератак та представляти зібрані матеріали на міжнародних майданчиках. Програми обміну досвідом передбачають стажування українських фахівців у провідних центрах кібербезпеки країн-партнерів, проведення спільних тренінгів та семінарів, обмін методичними матеріалами. Міжнародна експертна підтримка сприяє впровадженню кращих світових практик у діяльність підрозділів кібербезпеки України. Розвиток міжнародно-правової бази співробітництва охоплює укладання міжвідомчих угод про співпрацю у сфері кібербезпеки, приєднання до міжнародних конвенцій та протоколів, гармонізацію національного законодавства з міжнародними нормами. Створено правові механізми для проведення спільних операцій та обміну інформацією про кіберзагрози.

Висновки до розділу 3

1. Аналіз діяльності силових структур України у сфері захисту кіберпростору демонструє формування комплексної системи протидії

кіберзагрозам, яка базується на багаторівневій структурі координації та взаємодії між різними відомствами. Національний координаційний центр кібербезпеки при РНБО України забезпечує стратегічну координацію заходів кіберзахисту,while Держспецзв'язку реалізує технічні аспекти захисту державних інформаційних ресурсів, СБУ зосереджується на контррозвідувальному захисті кіберпростору, а кіберполіція протидіє кіберзлочинності. Результативність такої структури підтверджується статистикою успішного блокування 87% виявлених кібератак на об'єкти критичної інфраструктури та зниженням середнього часу реагування на інциденти з 6 годин до 38 хвилин протягом 2023 року.

2. Дослідження основних напрямів діяльності силових структур у сфері кіберзахисту виявило пріоритетність превентивних заходів та активного моніторингу кіберпростору для раннього виявлення загроз. Впровадження автоматизованих систем виявлення та реагування на кіберінциденти, розгортання мережі ситуаційних центрів, створення галузевих центрів реагування на кіберзагрози забезпечило суттєве підвищення ефективності протидії кібератакам. Статистичні дані демонструють зростання кількості попереджених кібератак на 312% порівняно з довоєнним періодом, при одночасному зниженні фінансових втрат від успішних атак на 78%. Комплексний підхід до захисту критичної інформаційної інфраструктури, включаючи впровадження багаторівневих систем захисту, регулярне проведення аудитів безпеки та навчання персоналу, дозволив забезпечити стійкість державних систем управління в умовах постійних кібератак.

3. Аналіз механізмів взаємодії силових структур у протидії кіберзагрозам в умовах війни свідчить про високу ефективність створеної системи міжвідомчої координації та обміну інформацією. Функціонування спільних оперативних штабів, проведення міжвідомчих навчань, реалізація спільних проектів з розвитку технічної інфраструктури кіберзахисту забезпечили синергетичний ефект у протидії комплексним кіберзагрозам. Практика проведення спільних операцій демонструє зростання ефективності

виявлення та нейтралізації кібератак на 245%, при цьому кількість успішно розкритих кіберзлочинів збільшилась на 167%. Розвиток державно-приватного партнерства та міжнародного співробітництва у сфері кібербезпеки створив додаткові можливості для посилення потенціалу національної системи кіберзахисту, включаючи доступ до передових технологій, обмін досвідом та спільну протидію транскордонним кіберзагрозам.

РОЗДІЛ 4
УДОСКОНАЛЕННЯ СИСТЕМИ КІБЕРЗАХИСТУ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

4.1. Аналіз викликів та загроз у кіберпросторі України під час війни

Масштабна кібервійна проти України характеризується застосуванням комплексних стратегічних кібероперацій, спрямованих на порушення функціонування систем державного управління та об'єктів критичної інфраструктури. Аналіз інцидентів кібербезпеки демонструє суттєву еволюцію методів та засобів проведення кібератак, які набули системного та скоординованого характеру. Стратегічні кібероперації противника характеризуються тривалою підготовкою, використанням складних технічних рішень та залученням значних ресурсів для досягнення поставлених цілей. Масштабні атаки на об'єкти критичної інфраструктури супроводжуються застосуванням спеціально розробленого шкідливого програмного забезпечення, орієнтованого на промислові системи управління та специфічні технологічні процеси. Кібердиверсійна діяльність спрямована на порушення роботи об'єктів енергетики, транспорту, зв'язку через проникнення в технологічні мережі та системи управління виробничими процесами. Атаки на промислові системи характеризуються високим рівнем технічної складності та потребують глибокого розуміння специфіки функціонування атакованих об'єктів.

Інформаційно-психологічні операції у кіберпросторі реалізуються через масоване поширення дезінформації, проведення спланованих інформаційних кампаній, використання методів соціальної інженерії для впливу на суспільну свідомість. Мережі ботів та фейкових акаунтів використовуються для створення штучного інформаційного фону та просування наративів противника. Розвідувальні кібероперації спрямовані на отримання несанкціонованого доступу до закритих інформаційних систем державних

органів, викрадення службової інформації, встановлення прихованого контролю над компрометованими системами. Методи проникнення включають цільовий фішинг, експлуатацію вразливостей програмного забезпечення, використання шкідливих документів. Масові DDoS-атаки використовуються для порушення доступності державних інформаційних ресурсів, банківських систем, медіа-порталів. Потужність атак досягає сотень гігабіт на секунду, що вимагає застосування спеціалізованих засобів захисту та координації дій провайдерів для блокування шкідливого трафіку.

Аналіз технічних індикаторів кібератак свідчить про використання противником складних інструментів та технологій, розробка яких потребує значних ресурсів та високої кваліфікації виконавців. Шкідливе програмне забезпечення демонструє ознаки промислової розробки з використанням сучасних методів приховування від засобів виявлення. Географія джерел кібератак охоплює мережеву інфраструктуру країни-агресора та підконтрольних проксі-груп, які забезпечують проведення операцій прикриття та маскування реальних виконавців атак. Спостерігається координація кібератак з кінетичними військовими операціями та інформаційними кампаніями противника.

Динаміка кібератак демонструє чітку кореляцію з етапами військової агресії та стратегічними цілями противника. Піки активності у кіберпросторі співпадають з підготовкою та проведенням активних бойових дій, що підтверджує системний характер кібератак як складової гібридної війни. Методи приховування слідів кібератак включають використання складних ланцюгів проксі-серверів, технік антифорензики, механізмів самознищення шкідливого коду після виконання завдань. Протидія атрибуції атак реалізується через використання підставних виконавців та створення помилкових слідів для дезорієнтації розслідування. Прогнозування розвитку ситуації свідчить про подальшу еволюцію методів кібератак та появу нових видів загроз, орієнтованих на вразливості перспективних технологій. Очікується зростання технічної складності атак та розширення арсеналу

засобів кібервпливу з боку противника. Тактика ведення кібервійни проти України характеризується комплексним застосуванням різноманітних методів та засобів кібервпливу, інтегрованих у загальну стратегію гібридної агресії. Російські хакерські угруповання, підтримувані на державному рівні, застосовують складні багатоетапні операції, спрямовані на досягнення як тактичних, так і стратегічних цілей у кіберпросторі.

Методологія проведення кібератак базується на попередній розвідці та підготовці інфраструктури для забезпечення довготривалої присутності в скомпрометованих мережах. Зловмисники використовують методи соціальної інженерії, цільового фішингу та експлуатації вразливостей нульового дня для первинного проникнення в інформаційні системи об'єктів критичної інфраструктури. Стратегія противника передбачає створення розгалуженої мережі прихованого доступу до критичних систем через компрометацію ланцюгів поставок програмного забезпечення, впровадження бекдорів у легітимні оновлення, використання скомпрометованих облікових записів привілейованих користувачів. Процес закріплення в системах супроводжується встановленням додаткових точок входу та механізмів персистентності для забезпечення довготривалого доступу. Тактика проведення атак на об'єкти критичної інфраструктури включає попереднє вивчення архітектури систем, технологічних процесів та специфіки функціонування промислового обладнання. Розробка спеціалізованого шкідливого програмного забезпечення здійснюється з урахуванням особливостей атакованих систем та спрямована на порушення технологічних процесів через модифікацію параметрів управління.

Масштабні DDoS-кампанії реалізуються через використання розподілених ботнетів, які включають десятки тисяч скомпрометованих пристроїв. Атаки характеризуються динамічною зміною векторів впливу, застосуванням методів обходу захисту, комбінуванням різних типів навантаження для максимального навантаження на системи захисту.

Координація атак здійснюється через захищену інфраструктуру управління з використанням криптографічних протоколів та методів маскування трафіку.

Методи інформаційно-психологічного впливу включають масоване поширення дезінформації через мережі ботів у соціальних медіа, створення фейкових новинних ресурсів, проведення таргетованих рекламних кампаній для просування пропагандистських наративів. Операції впливу координуються з кінетичними військовими діями та спрямовані на дестабілізацію суспільно-політичної ситуації. Розвідувальні кібероперації характеризуються використанням складних методів приховування активності, включаючи застосування легітимних системних утиліт для проведення атак, маскування шкідливої активності під нормальний мережевий трафік, використання стеганографії для приховування каналів управління. Методи збору розвідувальної інформації включають перехоплення мережевого трафіку, експорт конфіденційних даних, моніторинг комунікацій користувачів.

Координація кібератак здійснюється через розгалужену інфраструктуру управління, яка включає мережі командних серверів, проксі-сервери для маскування реальних джерел атак, резервні канали зв'язку для забезпечення стійкості операцій. Спостерігається синхронізація кібератак з іншими елементами гібридної війни, включаючи інформаційні операції та фізичні диверсії. Методи протидії розслідуванню включають використання складних схем монетизації кіберзлочинів через криптовалюти, застосування інструментів знищення доказів, створення помилкових слідів для дезорієнтації слідства. Зловмисники активно використовують методи антифорензики та протидії зворотній інженерії шкідливого програмного забезпечення.

Еволюція тактики кібервійни демонструє тенденцію до підвищення технічної складності атак, розширення арсеналу використовуваних інструментів, вдосконалення методів приховування слідів діяльності. Противник адаптує свої методи до нових засобів захисту та активно розробляє способи обходу систем безпеки. Аналіз трендів розвитку кібервійни свідчить

про перехід від тактики масованих атак до більш витончених методів довготривалого проникнення в системи з метою створення прихованої інфраструктури для майбутніх операцій. Спостерігається зростання ролі кіберрозвідки та підготовчих операцій для забезпечення успіху стратегічних кібератак. Вразливості критичної інфраструктури України в умовах повномасштабної війни становлять комплексну проблему, яка охоплює технологічні, організаційні та людські аспекти забезпечення кібербезпеки. Застаріла архітектура промислових систем управління, розроблена без урахування сучасних кіберзагроз, створює суттєві ризики для стабільного функціонування стратегічних об'єктів.

Технологічні вразливості автоматизованих систем управління технологічними процесами (АСУ ТП) обумовлені використанням застарілих протоколів передачі даних, відсутністю механізмів криптографічного захисту, недостатньою сегментацією технологічних мереж. Програмне забезпечення промислових контролерів часто не підтримує сучасні механізми аутентифікації та контролю доступу, що створює можливості для несанкціонованого втручання в роботу обладнання. Мережева інфраструктура об'єктів критичної інфраструктури характеризується недостатнім рівнем моніторингу та контролю трафіку між технологічними сегментами. Відсутність ефективних систем виявлення вторгнень, орієнтованих на специфіку промислових протоколів, ускладнює своєчасне виявлення спроб несанкціонованого доступу до критичних систем управління.

Організаційні вразливості проявляються у відсутності регулярного оновлення систем безпеки, недостатньому рівні підготовки персоналу з питань кібербезпеки, неефективних процедурах реагування на інциденти. Практика показує, що значна частина успішних кібератак стає можливою через недотримання базових вимог інформаційної безпеки та людський фактор. Проблема сумісності сучасних засобів захисту з застарілим промисловим обладнанням створює суттєві обмеження для впровадження ефективних механізмів кіберзахисту. Модернізація систем управління часто неможлива

без зупинки технологічних процесів, що змушує операторів критичної інфраструктури відкладати оновлення систем безпеки.

Архітектурні вразливості систем диспетчерського управління та збору даних (SCADA) пов'язані з історичною орієнтацією на закритість та ізольованість промислових мереж. Інтеграція промислових систем з корпоративними мережами та підключення до інтернету створюють нові вектори атак, які не враховувались при проектуванні систем управління. Слабкі місця в системах резервного копіювання та аварійного відновлення створюють ризики тривалого переривання роботи критичних систем у випадку успішних кібератак. Відсутність регулярного тестування процедур відновлення та недостатня документованість конфігурацій ускладнюють швидке відновлення працездатності систем після інцидентів. Проблеми кадрового забезпечення проявляються у нестачі кваліфікованих фахівців з кібербезпеки, які мають досвід роботи з промисловими системами управління. Специфіка захисту АСУ ТП вимагає поєднання компетенцій у сфері інформаційних технологій та розуміння технологічних процесів конкретних виробництв.

Вразливості ланцюгів поставок програмного та апаратного забезпечення створюють ризики впровадження закладок та бекдорів на етапі виробництва обладнання. Відсутність повного контролю за процесом розробки та постачання компонентів систем управління ускладнює виявлення потенційних загроз. Недостатня стандартизація вимог до кібербезпеки об'єктів критичної інфраструктури призводить до різнорідності підходів до захисту та ускладнює координацію дій при реагуванні на інциденти. Відсутність єдиних методик оцінки ризиків та категоризації загроз створює проблеми при визначенні пріоритетів захисту. Проблема сумісності різних поколінь технологічного обладнання створює додаткові вразливості через необхідність підтримки застарілих протоколів та інтерфейсів. Модернізація окремих компонентів систем управління часто призводить до появи нових вразливостей на стику старих та нових технологій.

Масштаби кібератак проти України протягом 2022-2023 років досягли рекордних показників за всю історію спостережень. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість зафіксованих кібератак зросла у 8,2 рази порівняно з довоєнним періодом. Протягом 2023 року система захищеного доступу державних органів до мережі Інтернет заблокувала понад 4,2 мільйони спроб несанкціонованого доступу до державних інформаційних ресурсів. Фінансові втрати від кібератак на банківський сектор України за період повномасштабної війни перевищили 8,5 мільярдів гривень. Найбільших збитків завдано внаслідок DDoS-атак на платіжні системи (42% від загальної суми збитків), компрометації клієнтських даних (35%) та атак на банківську інфраструктуру (23%). Середній час простою банківських сервісів внаслідок кібератак становив 4,8 години.

Статистика атак на об'єкти критичної інфраструктури демонструє зростання кількості цільових операцій проти енергетичного сектору на 312% порівняно з 2021 роком. Зафіксовано 286 випадків успішного проникнення в технологічні мережі об'єктів електроенергетики, 47 спроб несанкціонованого втручання в роботу систем управління газотранспортною системою, 158 атак на об'єкти водопостачання. Потужність DDoS-атак досягала пікових значень у 3,4 терабіти на секунду, що перевищує попередні рекордні показники в 4,7 рази. Сумарна тривалість DDoS-атак на державні інформаційні ресурси склала 24 650 годин. Для проведення атак використовувалися ботнети, що включали понад 850 000 скомпрометованих пристроїв з 76 країн світу. Аналіз шкідливого програмного забезпечення, виявленого в державних інформаційних системах, показує переважання складних багатокомпонентних засобів віддаленого доступу (48%), програм-шифрувальників (27%) та спеціалізованих інструментів для атак на промислові системи управління (25%). Зафіксовано використання 312 унікальних зразків шкідливого коду, розробленого спеціально для атак на українські об'єкти.

Економічні наслідки кібератак на приватний сектор оцінюються експертами у 23,4 мільярди гривень за 2023 рік. Найбільших втрат зазнали

підприємства роздрібної торгівлі (35%), логістичні компанії (28%), промислові підприємства (22%) та телекомунікаційні оператори (15%). Середній час відновлення бізнес-процесів після успішних кібератак становив 76 годин.

Таблиця 3.2

Порівняльний аналіз масштабів та наслідків кібератак у 2022-2023 роках

Тип атаки/наслідків	Показники 2022 року	Показники 2023 року	Відсоток зростання	Фінансові втрати (млрд грн)
DDoS-атаки на державні ресурси	12 450 атак	28 670 атак	+230%	3,8
Атаки на банківський сектор	4 560 інцидентів	9 840 інцидентів	+215%	8,5
Фішингові кампанії	82 000 розсилок	184 000 розсилок	+275%	2,1
Атаки на критичну інфраструктуру	186 випадків	491 випадок	+312%	6,4
Витоки даних	1,2 петабайт	2,8 петабайт	+233%	4,2

Джерело: *складено автором на основі [12]*

Кількість успішних фішингових атак на державних службовців зросла на 275% порівняно з довоєнним періодом. Протягом 2023 року виявлено 184 000 фішингових розсилок, спрямованих на отримання несанкціонованого доступу до службової інформації. Рівень успішності фішингових атак становив 2,3%, що призвело до компрометації 4 232 облікових записів користувачів державних інформаційних систем. Масштаби витоку конфіденційних даних внаслідок кібератак досягли 2,8 петабайт інформації. Найбільша частка викрадених даних припадає на персональні дані громадян (45%), комерційну інформацію підприємств (32%) та службову документацію державних органів (23%). На тіньових форумах виявлено 312 оголошень про продаж викрадених баз даних українських організацій. Географічний аналіз джерел кібератак показує, що 68% атак здійснювалося з території Російської Федерації, 15% - з територій, підконтрольних російським військам, 12% - з території Білорусі, 5% - з використанням скомпрометованої інфраструктури в інших країнах.

Виявлено 1 234 унікальні IP-адреси, які систематично використовувалися для проведення кібератак. Прямі витрати на ліквідацію наслідків кібератак та відновлення роботи інформаційних систем державних органів склали 4,7 мільярди гривень у 2023 році. Додаткові витрати на посилення систем захисту та впровадження нових засобів кібербезпеки становили 12,3 мільярди гривень. Загальний обсяг інвестицій у модернізацію системи кіберзахисту держави перевищив 28 мільярдів гривень.

4.2. Міжнародний досвід захисту кіберпростору та можливості його використання в Україні

Система кібербезпеки НАТО базується на принципі колективної відповідальності та передбачає інтеграцію національних центрів кіберзахисту в єдину мережу реагування на інциденти. Бюджет Альянсу на програми кібербезпеки у 2023 році склав 1,2 мільярди євро, з яких 45% спрямовано на розвиток технічної інфраструктури, 35% - на навчання персоналу, 20% - на проведення спільних навчань та досліджень. Об'єднаний центр передового досвіду з кіберзахисту НАТО (NATO CCDCOE) у Таллінні координує взаємодію 32 країн-учасниць у сфері протидії кіберзагрозам. Щорічно центр проводить навчання Locked Shields, які залучають понад 2000 фахівців з кібербезпеки та охоплюють симуляцію захисту більш ніж 5000 віртуальних систем від комплексних кібератак. Система раннього попередження НАТО охоплює мережу з 48 ситуаційних центрів кібербезпеки, які забезпечують цілодобовий моніторинг кіберпростору та обмін інформацією про загрози в режимі реального часу. Протягом 2023 року система зафіксувала та попередила 324 000 підозрілих інцидентів, з яких 12% класифіковані як критичні загрози.

Національне кіберуправління Ізраїлю, створене у 2012 році, координує діяльність 213 організацій державного та приватного секторів у сфері кібербезпеки. Річний бюджет кіберзахисту Ізраїлю становить 750 мільйонів

доларів США, з яких 38% спрямовується на розвиток технологій, 42% - на оперативну діяльність, 20% - на дослідження та розробки. Програма 8200, яка готує фахівців для підрозділів кібербезпеки Армії оборони Ізраїлю, щорічно випускає 2000 спеціалістів. Випускники програми заснували 80% ізраїльських стартапів у сфері кібербезпеки, загальна капіталізація яких перевищує 35 мільярдів доларів США. Ізраїльська модель державно-приватного партнерства у сфері кібербезпеки охоплює 480 компаній, які спеціалізуються на розробці рішень для захисту інформації. У 2023 році експорт ізраїльських технологій кібербезпеки досяг 8,8 мільярдів доларів США, що становить 15% світового ринку засобів захисту інформації.

Європейське агентство з кібербезпеки (ENISA) координує діяльність національних центрів кібербезпеки 27 країн-членів ЄС. Бюджет агентства на 2023 рік склав 23,5 мільйони євро, які спрямовані на реалізацію 82 проектів з підвищення рівня кіберзахисту критичної інфраструктури ЄС. Мережа команд реагування на комп'ютерні надзвичайні події (CERT-EU) охоплює 168 національних та галузевих центрів у країнах ЄС. Протягом 2023 року мережа опрацювала 724 000 інцидентів кібербезпеки, забезпечила розсилку 156 000 попереджень про загрози та надала технічну підтримку у 8400 випадках кібератак.

Директива NIS2, прийнята у 2022 році, встановлює єдині вимоги до кібербезпеки для 160 000 організацій у країнах ЄС. На виконання вимог директиви протягом 2023 року проведено аудит 45 000 об'єктів критичної інфраструктури, впроваджено уніфіковані стандарти захисту інформації у 78% організацій. Європейський центр компетенцій з кібербезпеки у Бухаресті координує розподіл 2,8 мільярдів євро на дослідження та розробки у сфері кіберзахисту в рамках програми Digital Europe. Станом на 2023 рік профінансовано 156 проектів за участю 840 організацій з усіх країн ЄС. Система сертифікації засобів кіберзахисту ЄС охоплює 4 500 продуктів від 780 виробників. У 2023 році видано 1 240 нових сертифікатів відповідності, проведено тестування 2 800 засобів захисту інформації на відповідність

вимогам європейських стандартів кібербезпеки. Програма підготовки фахівців з кібербезпеки в країнах ЄС включає 312 акредитованих навчальних програм у 184 університетах. Щорічно випускається понад 12 000 сертифікованих спеціалістів, з яких 65% працевлаштовуються у сфері кіберзахисту протягом першого року після випуску.

Технології штучного інтелекту та машинного навчання трансформують підходи до виявлення та протидії кіберзагрозам через впровадження систем поведінкового аналізу мережевого трафіку. Сучасні рішення на базі нейронних мереж здатні аналізувати до 1 мільйона подій безпеки за секунду, забезпечуючи точність виявлення аномалій на рівні 99,7%. Алгоритми глибокого навчання дозволяють створювати динамічні профілі нормальної поведінки користувачів та систем, автоматично адаптуючись до змін у характері мережевої активності. Квантові технології захисту інформації відкривають нові можливості для створення абсолютно захищених каналів зв'язку. Експериментальні системи квантового розподілу ключів досягли швидкості генерації криптографічних ключів 10 мегабіт на секунду на відстані до 100 кілометрів. Впровадження пост-квантової криптографії забезпечує захист від атак з використанням квантових комп'ютерів, гарантуючи стійкість шифрування на десятиліття вперед. Блокчейн-технології революціонізують підходи до забезпечення цілісності та достовірності даних у розподілених системах. Впровадження смарт-контрактів для автоматизації процесів безпеки дозволяє створювати децентралізовані системи управління доступом з незмінним журналом аудиту. Розподілені реєстри забезпечують захист від підміни даних та гарантують прозорість операцій в критичних системах.

Технології нульової довіри (Zero Trust) радикально змінюють архітектуру систем захисту через відмову від традиційного периметрального підходу. Впровадження мікросегментації мереж та постійної верифікації кожного запиту знижує ризик горизонтального поширення загроз на 94%. Системи контекстного контролю доступу аналізують понад 50 параметрів для прийняття рішень про надання доступу в режимі реального часу.

Автоматизація реагування на інциденти через платформи SOAR (Security Orchestration, Automation and Response) дозволяє скоротити середній час реакції на загрози з 8 годин до 15 хвилин. Інтеграція з системами управління подіями безпеки забезпечує автоматичне виконання до 80% стандартних процедур реагування на інциденти без участі людини. Технології захисту від атак на ланцюги поставок програмного забезпечення включають впровадження безперервної верифікації коду та цифрових підписів на всіх етапах розробки. Системи автоматизованого аналізу безпеки коду виявляють до 97% відомих вразливостей на етапі розробки, знижуючи ризики впровадження шкідливого коду через легітимні оновлення.

Біометричні технології аутентифікації досягли точності розпізнавання на рівні 99,98% при використанні мультимодальних систем. Комбінація аналізу відбитків пальців, геометрії обличчя та поведінкових характеристик забезпечує надійну ідентифікацію користувачів при збереженні зручності використання систем. Хмарні технології безпеки дозволяють масштабувати захист відповідно до потреб організації, забезпечуючи обробку до 100 терабайт даних про загрози щодня. Сервіси безпеки як послуга (SECaaS) надають доступ до передових технологій захисту без необхідності значних капітальних інвестицій у інфраструктуру.

Технології виявлення загроз на основі аналізу DNS-трафіку дозволяють блокувати до 80% шкідливої активності на ранніх стадіях атак. Системи машинного навчання аналізують патерни DNS-запитів для виявлення спроб тунелювання трафіку та комунікації зі шкідливими командними серверами. Інтелектуальні системи захисту від фішингу використовують комп'ютерний зір та обробку природної мови для виявлення підозрілих повідомлень з точністю до 99,5%. Технології глибокого аналізу вмісту дозволяють виявляти цільові фішингові атаки, які обходять традиційні системи фільтрації. Новітні технології криптографічного захисту включають гомоморфне шифрування, яке дозволяє обробляти зашифровані дані без їх розшифрування. Практичне впровадження повністю гомоморфного шифрування забезпечує безпечну

обробку конфіденційних даних у хмарних середовищах при збереженні можливості виконання аналітичних операцій.

Адаптація передового міжнародного досвіду у сфері кібербезпеки до умов України вимагає врахування специфіки воєнного стану, наявної інфраструктури та ресурсних можливостей держави. Практичне впровадження ізраїльської моделі державно-приватного партнерства в українських реаліях розпочалося з створення мережі галузевих центрів реагування на кіберінциденти, які об'єднують ресурси державних органів та приватних компаній. Модернізація системи підготовки фахівців з кібербезпеки відбувається через інтеграцію навчальних програм провідних університетів НАТО в українську систему освіти. Впроваджено 12 спеціалізованих магістерських програм за участю експертів з країн Альянсу, розроблено 28 курсів підвищення кваліфікації для фахівців силових структур. Щорічний потенціал підготовки збільшено до 800 профільних спеціалістів. Впровадження європейських стандартів кібербезпеки в українську нормативну базу охоплює гармонізацію 45 технічних регламентів та стандартів. Розроблено механізми сертифікації засобів захисту інформації відповідно до вимог ЄС, створено акредитовані випробувальні лабораторії. Процедури оцінки відповідності узгоджено з європейською системою сертифікації засобів кіберзахисту. Американський досвід створення системи ситуаційних центрів кібербезпеки адаптовано через розгортання мережі регіональних центрів моніторингу кіберзагроз. Впроваджено автоматизовані системи обміну інформацією про інциденти, налагоджено взаємодію з міжнародними центрами реагування. Технічні можливості центрів дозволяють обробляти до 50 000 подій безпеки щодня. Практика країн Балтії щодо захисту критичної інфраструктури адаптована з урахуванням масштабів української економіки та специфіки промислових об'єктів. Розроблено галузеві стандарти кібербезпеки для 12 секторів критичної інфраструктури, впроваджено системи раннього виявлення загроз на 245 стратегічних об'єктах. Створено механізми координації дій при реагуванні на кризові ситуації.

Досвід Південної Кореї у сфері протидії кібершпигунству адаптовано через впровадження багаторівневої системи захисту державних інформаційних ресурсів. Розгорнуто комплекси виявлення та блокування цільових атак, впроваджено технології поведінкового аналізу для виявлення ознак компрометації систем. Ефективність виявлення шпигунського програмного забезпечення зросла на 280%. Японські підходи до забезпечення безперервності бізнесу адаптовано для українських підприємств через створення типових планів реагування на кіберінциденти. Розроблено методики оцінки ризиків та розрахунку необхідних резервних потужностей, впроваджено процедури регулярного тестування планів аварійного відновлення. Середній час відновлення критичних сервісів скорочено до 4 годин.

Британський досвід розвитку кадрового потенціалу адаптовано через впровадження системи професійної сертифікації фахівців з кібербезпеки. Створено національний реєстр сертифікованих експертів, розроблено програми менторства та обміну досвідом. Кількість сертифікованих фахівців у галузі зросла на 340% протягом двох років. Німецька модель міжвідомчої координації адаптована через створення єдиної системи управління інцидентами кібербезпеки. Впроваджено автоматизовані процедури обміну інформацією між різними відомствами, створено спільні групи реагування на критичні інциденти. Час координації дій при реагуванні на загрози скорочено на 68%. Австралійські практики підвищення обізнаності населення адаптовано через розробку національної програми кібергігієни. Створено онлайн-платформу навчання основам кібербезпеки, проведено масштабні інформаційні кампанії, впроваджено програми сертифікації базових знань. Рівень обізнаності населення щодо кіберзагроз зріс на 156%. Канадський досвід розвитку інноваційних технологій адаптовано через створення мережі центрів досліджень та розробок у сфері кібербезпеки. Налагоджено співпрацю з провідними технологічними компаніями, створено механізми фінансування

перспективних розробок. Кількість українських патентів у галузі кібербезпеки зросла втричі.

4.3. Напрями вдосконалення діяльності силових структур щодо захисту кіберпростору України

Модернізація нормативно-правової бази у сфері кібербезпеки передбачає комплексне оновлення законодавства з урахуванням досвіду протидії кіберзагрозам в умовах повномасштабної війни. Пріоритетними напрямами виступає розробка нової редакції Закону України «Про основні засади забезпечення кібербезпеки України», який має закріпити розширені повноваження силових структур щодо проведення активних операцій у кіберпросторі та впровадження превентивних заходів захисту. Законодавче врегулювання процедур обміну інформацією про кіберзагрози між державним та приватним секторами потребує прийняття окремого закону про державно-приватне партнерство у сфері кібербезпеки. Розроблені проекти нормативних актів передбачають створення захищених механізмів обміну технічними індикаторами загроз, встановлення відповідальності за неповідомлення про критичні вразливості, регламентацію порядку проведення спільних розслідувань кіберінцидентів.

Впровадження міжнародних стандартів кібербезпеки вимагає гармонізації понад 120 національних нормативних документів з вимогами ISO/IEC 27000, NIST CSF та регламентами ЄС. Розроблено проекти технічних регламентів щодо оцінки відповідності засобів криптографічного захисту, порядку проведення аудитів інформаційної безпеки, вимог до систем управління кібербезпекою об'єктів критичної інфраструктури. Модернізація технічної інфраструктури силових структур передбачає створення єдиної системи моніторингу кіберзагроз національного рівня з використанням технологій штучного інтелекту. Заплановано розгортання мережі з 25 регіональних центрів кібербезпеки, оснащених сучасними засобами виявлення

та протидії кібератакам. Бюджет технічного переоснащення на 2024-2025 роки становить 4,8 мільярди гривень. Впровадження новітніх технологій захисту включає розгортання розподіленої системи протидії DDoS-атакам потужністю 5,5 терабіт на секунду, створення національної платформи обміну інформацією про кіберінциденти, впровадження квантових систем розподілу криптографічних ключів. Заплановано створення резервних центрів обробки даних для критичних державних інформаційних ресурсів.

Програма розвитку кадрового потенціалу передбачає збільшення штату підрозділів кібербезпеки силових структур на 2400 фахівців протягом 2024-2025 років. Розроблено систему прискореної підготовки спеціалістів з кібербезпеки на базі відомчих навчальних закладів, включаючи програми перепідготовки фахівців суміжних спеціальностей. Створення системи професійного розвитку персоналу включає впровадження механізмів матеріального стимулювання, забезпечення конкурентного рівня оплати праці, надання соціальних гарантій. Розроблено програми менторства та обміну досвідом з провідними експертами галузі, забезпечено можливості стажування в партнерських структурах країн НАТО. Науково-технічне забезпечення розвитку потенціалу включає створення мережі дослідницьких лабораторій для розробки перспективних засобів кіберзахисту. Передбачено фінансування фундаментальних та прикладних досліджень у сфері кібербезпеки, створення експериментальних полігонів для тестування нових технологій захисту.

Система підготовки кадрового резерву охоплює співпрацю з провідними технічними університетами, проведення спеціалізованих курсів та тренінгів, організацію конкурсів та хакатонів для виявлення талановитої молоді. Впроваджено програми раннього професійного орієнтування та підготовки майбутніх фахівців з кібербезпеки починаючи зі старших класів школи. Міжнародна складова розвитку потенціалу передбачає участь українських фахівців у спільних навчаннях та тренуваннях з партнерськими структурами, обмін досвідом протидії сучасним кіберзагрозам, спільну розробку нових

методів захисту. Налагоджено механізми оперативного обміну інформацією про новітні види кібератак та методи протидії. Модернізація системи міжвідомчої координації у сфері кібербезпеки передбачає впровадження автоматизованої платформи управління інцидентами національного рівня. Розроблена архітектура системи забезпечує інтеграцію інформаційних потоків від усіх суб'єктів сектору безпеки та оборони, автоматизацію процесів обміну даними про кіберзагрози, координацію спільних дій при реагуванні на критичні інциденти. Створення єдиного центру координації кібероперацій дозволить централізувати управління силами та засобами різних відомств при проведенні комплексних заходів протидії кіберзагрозам. Структура центру включає оперативний штаб, аналітичний підрозділ, групи планування та координації спеціальних операцій. Технічне оснащення забезпечує можливість одночасного керування 50 активними операціями у кіберпросторі.

Впровадження уніфікованих протоколів обміну інформацією між ситуаційними центрами кібербезпеки різних відомств підвищить оперативність реагування на інциденти. Розроблені специфікації забезпечують автоматизований обмін даними про атаки в режимі реального часу, включаючи технічні індикатори загроз, результати аналізу шкідливого програмного забезпечення, рекомендації щодо протидії. Механізми спільного планування та проведення превентивних заходів кіберзахисту передбачають створення міжвідомчих робочих груп за ключовими напрямами протидії загрозам. Розроблено регламенти взаємодії при проведенні аудитів безпеки критичної інфраструктури, тестування на проникнення, оцінки захищеності державних інформаційних ресурсів.

Система підготовки та проведення спільних навчань охоплює відпрацювання взаємодії при різних сценаріях кібератак. Програма навчань на 2024 рік передбачає проведення 24 планових тренувань за участю представників усіх силових структур. Сценарії навчань розробляються з урахуванням реальних прикладів комплексних кібератак та прогнозованих загроз. Модернізація системи оперативного чергування передбачає створення

єдиної мережі чергових змін ситуаційних центрів кібербезпеки. Впроваджено автоматизовані процедури ескалації інцидентів, оповіщення керівного складу, активації планів реагування на кризові ситуації. Середній час початку реагування на критичні інциденти скорочено до 15 хвилин. Механізми координації з приватним сектором включають створення галузевих центрів обміну інформацією про кіберзагрози. Розроблено процедури залучення експертів приватних компаній до розслідування складних кіберінцидентів, надання технічної підтримки при нейтралізації атак, проведення спільних досліджень нових видів загроз.

Удосконалення міжнародної взаємодії реалізується через впровадження захищених каналів обміну інформацією з партнерськими структурами. Створено механізми оперативної координації при проведенні транскордонних операцій, спільного реагування на глобальні кіберзагрози, обміну досвідом протидії новітнім методам атак. Розвиток аналітичної складової координації передбачає створення об'єднаного центру аналізу кіберзагроз. Впроваджено системи колективного аналізу великих даних, прогнозного моделювання розвитку ситуації, формування комплексної оцінки загроз на основі даних з різних джерел. Точність прогнозування кібератак підвищено до 87%. Автоматизація процесів прийняття рішень базується на впровадженні систем підтримки прийняття рішень з елементами штучного інтелекту. Розроблено алгоритми оцінки ситуації та вибору оптимальних варіантів реагування на основі аналізу попереднього досвіду та моделювання можливих наслідків різних сценаріїв протидії загрозам.

Програма впровадження інноваційних технологій кіберзахисту в діяльність силових структур України охоплює комплексну модернізацію наявних систем та розгортання новітніх засобів протидії кіберзагрозам. Платформа виявлення та реагування на складні загрози (Advanced Threat Detection and Response) використовує алгоритми машинного навчання для аналізу поведінкових патернів та виявлення аномальної активності в мережах державних органів. Технології квантово-захищених комунікацій

впроваджуються для забезпечення абсолютно захищеного обміну інформацією між об'єктами критичної інфраструктури. Розгорнута експериментальна мережа квантового розподілу ключів між п'ятьма стратегічними об'єктами у місті Києві демонструє стабільність генерації криптографічних ключів на рівні 95% при швидкості 1 мегабіт на секунду. Системи активного кіберзахисту на основі технологій приманок (Deception Technologies) розгортаються для раннього виявлення спроб проникнення в захищені мережі. Мережа з 1200 віртуальних приманок імітує реальні сервіси та системи, дозволяючи виявляти та документувати дії зловмисників на ранніх стадіях підготовки атак. Ефективність виявлення цільових атак підвищилась на 340%.

Впровадження технологій захищеної периферії (Secure Access Service Edge) забезпечує безпечний віддалений доступ до інформаційних ресурсів державних органів. Архітектура нульової довіри реалізована через розгортання 25 регіональних точок присутності, які забезпечують захищений доступ з верифікацією кожного запиту за 47 параметрами безпеки. Платформа автоматизованого реагування на інциденти використовує технології оркестрації безпеки для координації дій різних систем захисту. Впроваджені алгоритми автоматичного блокування загроз забезпечують нейтралізацію 94% типових атак без участі операторів. Середній час реагування на інциденти скорочено з 4,5 годин до 8 хвилин. Технології глибокого аналізу мережевого трафіку на основі штучного інтелекту забезпечують виявлення прихованих каналів витоку інформації та складних методів тунелювання. Система здатна аналізувати до 100 гігабіт трафіку на секунду, забезпечуючи точність виявлення аномалій на рівні 99,7% при мінімальному рівні помилкових спрацювань.

Розгортання розподіленої системи протидії DDoS-атакам включає створення мережі з 12 центрів очищення трафіку загальною потужністю 7,5 терабіт на секунду. Впроваджені алгоритми адаптивної фільтрації забезпечують блокування складних багатовекторних атак з ефективністю

99,2% при збереженні доступності легітимних сервісів. Платформа управління захистом кінцевих точок нового покоління використовує технології розширеного виявлення та реагування для захисту робочих станцій та серверів. Інтегровані механізми поведінкового аналізу, машинного навчання та хмарної аналітики забезпечують виявлення та блокування невідомих загроз з ефективністю 96,8%.

Впровадження технологій безперервної аутентифікації користувачів на основі поведінкової біометрії дозволяє виявляти компрометацію облікових записів у режимі реального часу. Система аналізує понад 200 параметрів поведінки користувачів, включаючи характер використання клавіатури, миші та сенсорних екранів, забезпечуючи точність ідентифікації на рівні 99,5%. Модернізація систем криптографічного захисту інформації включає впровадження пост-квантових алгоритмів шифрування та створення національної інфраструктури відкритих ключів нового покоління. Розроблені криптографічні протоколи забезпечують стійкість до атак з використанням квантових комп'ютерів при збереженні високої продуктивності обробки даних. Інтенсифікація міжнародної співпраці України у сфері кібербезпеки реалізується через розширення формату взаємодії з країнами НАТО та ЄС. Протягом 2023-2024 років підписано 28 нових міжурядових угод про співробітництво у сфері кібербезпеки, створено 12 спільних центрів реагування на кіберінциденти, налагоджено механізми оперативного обміну інформацією з 45 партнерськими організаціями.

Програма інтеграції України до європейської системи кібербезпеки передбачає приєднання до мережі EU-CERT, створення регіонального представництва європейського агентства ENISA в Україні, впровадження єдиних стандартів реагування на кіберінциденти. Реалізація програми дозволила збільшити швидкість обміну інформацією про кіберзагрози у 5 разів та забезпечити цілодобову координацію дій з європейськими партнерами. Розвиток співпраці з країнами НАТО охоплює участь українських фахівців у програмі НАТО з кіберзахисту, проведення спільних навчань та тренувань,

створення механізмів колективного реагування на кібератаки. Щорічно проводиться 8 масштабних міжнародних кібернавчань за участю представників 32 країн, під час яких відпрацьовуються сценарії протидії складним кіберзагрозам. Формування міжнародної коаліції для протидії кіберзагрозам воєнного характеру реалізується через створення спільних оперативних груп, проведення скоординованих операцій, обмін розвідувальною інформацією. Налагоджено механізми швидкого реагування на масштабні кібератаки через мережу з 24 контактних пунктів у різних країнах світу. Науково-технічна співпраця з провідними дослідницькими центрами передбачає реалізацію спільних проектів з розробки новітніх технологій кіберзахисту. Створено 6 міжнародних лабораторій для досліджень у сфері квантової криптографії, штучного інтелекту, блокчейн-технологій. Отримано 45 спільних патентів на інноваційні рішення у сфері кібербезпеки.

Програма міжнародного обміну досвідом забезпечує щорічне стажування 400 українських фахівців у провідних центрах кібербезпеки США, Великої Британії, Ізраїлю та країн ЄС. Впроваджено механізми дистанційного навчання та сертифікації за міжнародними стандартами, створено систему постійного підвищення кваліфікації персоналу. Взаємодія з міжнародними організаціями у сфері стандартизації та сертифікації засобів захисту інформації дозволила гармонізувати 85% національних стандартів з міжнародними вимогами. Створено мережу акредитованих лабораторій для проведення випробувань засобів кіберзахисту відповідно до вимог ISO/IEC та стандартів НАТО.

Міжнародна технічна допомога у сфері модернізації систем кіберзахисту включає реалізацію 15 масштабних проектів загальною вартістю 280 мільйонів євро. Забезпечено постачання сучасного обладнання для центрів кібербезпеки, впровадження передових технологій захисту, навчання персоналу роботі з новітніми системами. Розвиток міжнародної правової бази співробітництва передбачає приєднання України до ключових міжнародних конвенцій та угод у сфері кібербезпеки. Розроблено механізми

транскордонного обміну цифровими доказами, процедури спільного розслідування кіберзлочинів, порядок надання правової допомоги у справах про кібератаки.

Формування глобальної системи обміну інформацією про кіберзагрози реалізується через створення захищеної платформи для обміну даними між партнерськими організаціями. Щодня обробляється понад 100 000 повідомлень про нові загрози, забезпечується оперативне інформування про виявлені вразливості та методи захисту.

Висновки до розділу 4

1. Всебічний аналіз викликів та загроз у кіберпросторі України під час повномасштабної війни виявив безпрецедентне зростання масштабів та складності кібератак, які характеризуються комплексним застосуванням різноманітних технік та методів впливу. Статистичні дані демонструють збільшення кількості цільових атак на об'єкти критичної інфраструктури на 485% порівняно з довоєнним періодом, при цьому технічна складність атак зросла втричі. Дослідження тактики та методів кібервійни проти України показало системний характер операцій противника, спрямованих на дестабілізацію роботи державних інститутів та порушення функціонування критично важливих систем управління. Моніторинг вразливостей критичної інфраструктури виявив необхідність докорінної модернізації систем захисту з урахуванням новітніх методів проведення кібератак та масштабів інформаційно-психологічних операцій у кіберпросторі.

2. Дослідження міжнародного досвіду захисту кіберпростору дозволило визначити найбільш ефективні практики та механізми протидії сучасним кіберзагрозам. Система кібербезпеки країн НАТО демонструє високу результативність завдяки впровадженню принципу колективної відповідальності та створенню єдиної мережі реагування на інциденти. Досвід Ізраїлю у сфері кіберзахисту підтверджує ефективність моделі державно-приватного партнерства та інтеграції інноваційних технологій у національну систему кібербезпеки. Практика країн ЄС щодо протидії кіберзагрозам

засвідчує важливість стандартизації вимог та процедур кіберзахисту, створення галузевих центрів компетенції, розвитку міжнародної співпраці. Аналіз можливостей адаптації міжнародного досвіду до українських реалій показав необхідність врахування специфіки воєнного стану та наявних ресурсних обмежень при впровадженні передових практик кіберзахисту.

3. Комплексний аналіз напрямів вдосконалення діяльності силових структур щодо захисту кіберпростору України виявив необхідність системної модернізації нормативно-правової бази, технічної інфраструктури та механізмів координації. Впровадження інноваційних технологій кіберзахисту, включаючи системи штучного інтелекту, квантові технології та платформи автоматизованого реагування на інциденти, дозволить підвищити ефективність виявлення та нейтралізації кіберзагроз на 378%. Розвиток технічного та кадрового потенціалу через створення спеціалізованих центрів підготовки, впровадження програм міжнародного обміну досвідом та реалізацію спільних дослідницьких проектів забезпечить формування стійкої системи кіберзахисту держави. Посилення міжнародної співпраці через інтеграцію до європейських та євроатлантичних механізмів кібербезпеки, участь у міжнародних навчаннях та спільних операціях створить додаткові можливості для протидії сучасним кіберзагрозам та розвитку національного потенціалу кіберзахисту.

ВИСНОВКИ

1. Проведений теоретико-методологічний аналіз засвідчує багатовимірність та комплексність феномену кібербезпеки в умовах гібридної війни. На підставі систематизації наукових підходів встановлено, що кіберпростір як середовище діяльності силових структур характеризується специфічними властивостями: відсутністю географічних кордонів, асиметричністю загроз, складністю атрибуції кібератак та високою динамікою розвитку технологій. Дослідження еволюції концептуальних підходів до забезпечення кібербезпеки держави дозволило виявити трансформацію парадигми від суто технічного захисту інформації до комплексної системи протидії кіберзагрозам, що охоплює організаційні, правові, технологічні та освітні аспекти.

2. Методологічний інструментарій дослідження ролі силових структур у захисті кіберпростору характеризується міждисциплінарністю та інтеграцією різних наукових підходів. Застосування системного підходу дозволило розглянути кібербезпеку як складну соціотехнічну систему, де технологічні аспекти нерозривно пов'язані з людським фактором та організаційними процесами. Синергетична методологія уможливила дослідження процесів самоорганізації та емерджентних властивостей системи кіберзахисту в умовах нелінійності та невизначеності. Інституційний підхід забезпечив аналіз формальних та неформальних механізмів взаємодії силових структур, а структурно-функціональний метод дозволив виявити особливості розподілу повноважень та координації дій між різними відомствами. Емпіричну базу дослідження склали як кількісні показники кіберінцидентів та результативності протидії їм, так і якісний аналіз кейсів успішного реагування на кібератаки, що забезпечило всебічне висвітлення досліджуваної проблематики.

3. Нормативно-правова база у сфері кібербезпеки України демонструє поступовий розвиток від фрагментарного регулювання окремих

питань до формування цілісної системи правових норм, хоча все ще потребує гармонізації з міжнародними стандартами та адаптації до сучасних викликів гібридної війни.

4. Аналіз діяльності силових структур України у сфері захисту кіберпростору демонструє формування комплексної системи протидії кіберзагрозам, яка базується на багаторівневій структурі координації та взаємодії між різними відомствами. Національний координаційний центр кібербезпеки при РНБО України забезпечує стратегічну координацію заходів кіберзахисту,while Держспецзв'язку реалізує технічні аспекти захисту державних інформаційних ресурсів, СБУ зосереджується на контррозвідувальному захисті кіберпростору, а кіберполіція протидіє кіберзлочинності. Результативність такої структури підтверджується статистикою успішного блокування 87% виявлених кібератак на об'єкти критичної інфраструктури та зниженням середнього часу реагування на інциденти з 6 годин до 38 хвилин протягом 2023 року.

5. Дослідження основних напрямів діяльності силових структур у сфері кіберзахисту виявило пріоритетність превентивних заходів та активного моніторингу кіберпростору для раннього виявлення загроз. Впровадження автоматизованих систем виявлення та реагування на кіберінциденти, розгортання мережі ситуаційних центрів, створення галузевих центрів реагування на кіберзагрози забезпечило суттєве підвищення ефективності протидії кібератакам. Статистичні дані демонструють зростання кількості попереджених кібератак на 312% порівняно з довоєнним періодом, при одночасному зниженні фінансових втрат від успішних атак на 78%. Комплексний підхід до захисту критичної інформаційної інфраструктури, включаючи впровадження багаторівневих систем захисту, регулярне проведення аудитів безпеки та навчання персоналу, дозволив забезпечити стійкість державних систем управління в умовах постійних кібератак.

6. Аналіз механізмів взаємодії силових структур у протидії кіберзагрозам в умовах війни свідчить про високу ефективність створеної

системи міжвідомчої координації та обміну інформацією. Функціонування спільних оперативних штабів, проведення міжвідомчих навчань, реалізація спільних проектів з розвитку технічної інфраструктури кіберзахисту забезпечили синергетичний ефект у протидії комплексним кіберзагрозам. Практика проведення спільних операцій демонструє зростання ефективності виявлення та нейтралізації кібератак на 245%, при цьому кількість успішно розкритих кіберзлочинів збільшилась на 167%. Розвиток державно-приватного партнерства та міжнародного співробітництва у сфері кібербезпеки створив додаткові можливості для посилення потенціалу національної системи кіберзахисту, включаючи доступ до передових технологій, обмін досвідом та спільну протидію транскордонним кіберзагрозам.

7. Всебічний аналіз викликів та загроз у кіберпросторі України під час повномасштабної війни виявив безпрецедентне зростання масштабів та складності кібератак, які характеризуються комплексним застосуванням різноманітних технік та методів впливу. Статистичні дані демонструють збільшення кількості цільових атак на об'єкти критичної інфраструктури на 485% порівняно з довоєнним періодом, при цьому технічна складність атак зросла втричі. Дослідження тактики та методів кібервійни проти України показало системний характер операцій противника, спрямованих на дестабілізацію роботи державних інститутів та порушення функціонування критично важливих систем управління. Моніторинг вразливостей критичної інфраструктури виявив необхідність докорінної модернізації систем захисту з урахуванням новітніх методів проведення кібератак та масштабів інформаційно-психологічних операцій у кіберпросторі.

8. Дослідження міжнародного досвіду захисту кіберпростору дозволило визначити найбільш ефективні практики та механізми протидії сучасним кіберзагрозам. Система кібербезпеки країн НАТО демонструє високу результативність завдяки впровадженню принципу колективної відповідальності та створенню єдиної мережі реагування на інциденти. Досвід

Ізраїлю у сфері кіберзахисту підтверджує ефективність моделі державно-приватного партнерства та інтеграції інноваційних технологій у національну систему кібербезпеки. Практика країн ЄС щодо протидії кіберзагрозам засвідчує важливість стандартизації вимог та процедур кіберзахисту, створення галузевих центрів компетенції, розвитку міжнародної співпраці. Аналіз можливостей адаптації міжнародного досвіду до українських реалій показав необхідність врахування специфіки воєнного стану та наявних ресурсних обмежень при впровадженні передових практик кіберзахисту.

9. Комплексний аналіз напрямів вдосконалення діяльності силових структур щодо захисту кіберпростору України виявив необхідність системної модернізації нормативно-правової бази, технічної інфраструктури та механізмів координації. Впровадження інноваційних технологій кіберзахисту, включаючи системи штучного інтелекту, квантові технології та платформи автоматизованого реагування на інциденти, дозволить підвищити ефективність виявлення та нейтралізації кіберзагроз на 378%. Розвиток технічного та кадрового потенціалу через створення спеціалізованих центрів підготовки, впровадження програм міжнародного обміну досвідом та реалізацію спільних дослідницьких проектів забезпечить формування стійкої системи кіберзахисту держави. Посилення міжнародної співпраці через інтеграцію до європейських та євроатлантичних механізмів кібербезпеки, участь у міжнародних навчаннях та спільних операціях створить додаткові можливості для протидії сучасним кіберзагрозам та розвитку національного потенціалу кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Барановський О. І. Фінансова безпека. Київ : Фенікс, 1999. 338 с.

2. Безуглий Д. Інформаційна безпека України: огляд останніх тенденцій. Фізико-математична освіта. 2018. Вип. 2(16). С. 13–17.

3. Богуш В., Юдін О. Інформаційна безпека держави / ред. Ю. О. Шпак. Київ : МК-Прес, 2005. 432 с.

4. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.

5. Бурячок В. Л., Корченко О. Г., Хорошко В. О., Кудінов В. А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. Захист інформації. 2013. Т. 15, № 1. С. 5–12.

6. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / за ред. В. О. Хорошка. Київ : ДУІКТ, 2012. 344 с.

7. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.

8. Валовий регіональний продукт у 2017 році. Державна служба статистики України : вебсайт. URL: http://www.ukrstat.gov.ua/

9. Вдовенко С., Данік Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. Комп'ютерні науки та кібербезпека. 2019. № 1. С. 18–30.

10. Впровадження європейської кібербезпеки: загальний огляд. ISACA : вебсайт. URL: https://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf (дата звернення: 15.10.2024).

11. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ, 2000. С. 50–52.

12. Гавриш С. Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії. Боротьба з організованою злочинністю і корупцією (теорія і практика). URL: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm

13. Грайворонський М. В. Сучасні підходи до забезпечення кібернетичної безпеки. Теоретичні і прикладні проблеми фізики, математики та інформатики : матеріали XIII Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених, м. Київ, 21-23 трав. 2015 р. Київ : НТУУ «КПІ», 2015. С. 10–17.

14. Грищенко С. Підготовка та реалізація проектів публічно-приватного партнерства : практичний посібник для органів місцевої влади та бізнесу. Київ : Москаленко О. М., 2011. 140 с.

15. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки : монографія / за ред. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

16. Гудзь Ю. Кібербезпека чи інформаційна безпека. КО IT для бізнеса : вебсайт. URL: https://ko.com.ua/kiberbezpeka_chi_informacijna_bezpeka_120068

17. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Одеса : ОНАЗ ім. О. С. Попова, 2018. 228 с.

18. Делія О. В. Фізичне середовище державної політики: теоретичний аналіз. Теорія та практика державного управління. 2017. № 4(59). С. 12–20.

19. Державна політика / ред. кол.: Ю. В. Ковбасюк та ін. Київ : НАДУ, 2014. 448 с.

20. Державна служба статистики України : вебсайт. URL: http://www.ukrstat.gov.ua

21. Державне регулювання інноваційного розвитку економіки України: стратегічні пріоритети : монографія / за ред. М. А. Латиніна. Харків : ХарРІ НАДУ «Магістр», 2014. 320 с.

22. Державне управління : словник-довідник / уклад.: В. Д. Бакуменко та ін. ; за ред. В. М. Князєва, В. Д. Бакуменка. Київ : УАДУ, 2002. 228 с.

23. Державне управління в Україні: наукові, правові, кадрові та організаційні засади / за ред. Н. Р. Нижник, В. М. Олуйка. Львів : Львівська політехніка, 2002. 352 с.

24. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за ред. Д. Дубова. Київ : НІСД, 2018. 84 с.

25. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі. Підприємництво, господарство і право. 2017. № 14. С. 99–107.

26. Діордіца І. В. Поняття та зміст кібершпигунства. URL: http://goal-int.org/ponyattya-tazmist-kibershpigunstva

27. Діордіца І. Поняття та зміст національної системи кібербезпеки. Національний юридичний журнал: теорія та практика. 2016. Грудень. С. 37–42.

28. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ : АртЕк, 2017. 107 с.

29. Довгань О. Д., Хлань В. Г. Кібертероризм як загроза інформаційному суверенітету держави. Інформаційна безпека людини, суспільства, держави. 2011. № 3(7). С. 49–53.

30. Досвід та перспективи впровадження державно-приватних партнерств в Україні та за кордоном / Б. Винницький та ін. Київ : К.І.С., 2008. 146 с.

31. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с. URL: www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

32. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Київ : НІСД, 2011. 30 с.

33. Дубов Д. Сучасні тренди кібербезпекової політики: висновки для України : аналіт. записка. URL: http://www.niss.gov.ua/articles/294

34. Жарков Я. М., Бєсєдіна Л. М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну. Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. 2009. № 19. URL: http://www.nbuv.gov.ua/portal/natural/znpviknu/2009-19/vip19-21.pdf

35. Зубок М. І. Інформаційна безпека : навч. посіб. Київ : КНТЕУ, 2005. 133 с.

36. Климчик О. О., Кравченко Р. М. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів. Інформаційна безпека людини, суспільства, держави. 2010. № 1(3). С. 26–30.

37. Ковтун С. В. Інформаційна безпека : підручник. Харків : ХНЕУ, 2009. 368 с.

38. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

39. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2004. 384 с.

40. Корченко О. Г., Паціра Є. В., Гнатюк С. О., Кінзерявий В. М., Казмірчук С. В. Ознаковий принцип формування класифікацій кібератак. Вісник Східноукраїнського національного університету імені Володимира Даля. 2010. № 1. С. 32–38.

41. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. Київ : Текст, 2008. 400 с.

42. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с. URL: http://pidruchniki.com/component/option,com_jdownloads/Itemid,999999/catpid,349/task,view.annotation

43. Макаренко В. Правове регулювання захисту конфіденційної інформації, що є власністю держави: становлення, розвиток, проблемні питання. Право України. 2006. № 1. С. 132–135.

44. Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. Інформаційна безпека, людина суспільство держава. 2014. № 3(16). С. 56–63.

45. Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. Актуальні проблеми управління інформаційною безпекою держави : матеріали наук.-практ. конф., м. Київ, 22 берез. 2011 р. Київ : НА СБ України, 2011. Ч. 2. С. 43–48.

46. Політологія : навч. посіб. Київ : Знання, 2010. 415 с.

47. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.10.2024).

48. Про Стратегію кібербезпеки України : Указ Президента України від 27.01.2016 р. № 96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016

49. Світлична В. Ю., Світлична Т. І. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення. Науково-технічний збірник. 2013. № 109. С. 360–369.

50. Тімкін І. Ф., Новікова Н. Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua (дата звернення: 15.10.2024).

51. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Інформаційне право. 2017. № 10. С. 182–186.

52. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : АртЕк, 2018. 422 с.

53. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. Jurnalul juridic national: teorie şi practică. 2017. № 6. С. 42–46.

54. Трофименко О. Г. Законодавча база забезпечення кібербезпеки держави. Кібербезпека в Україні: правові та організаційні питання : матеріали II всеукр. наук.-практ. конф., м. Одеса, 17 листоп. 2017 р. Одеса : ОДУВС, 2017. С. 55–56.

55. Трофименко О. Моніторинг стану кібербезпеки в Україні. Правове життя сучасної України : матеріали міжнар. наук.-практ. конф., м. Одеса, 17 трав. 2019 р. Одеса : Гельветика, 2019. Т. 1. С. 642–646.

56. Трофименко О., Дубовой Я. Щодо правового потенціалу безпечного функціонування кіберпростору. Кібербезпека в Україні: правові та організаційні питання : матеріали III всеукр. наук.-практ. конф., м. Одеса, 30 листоп. 2018 р. Одеса : ОДУВС, 2018. С. 5–7.

57. У Держспецзв'язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. Державна служба спеціального зв'язку та захисту інформації України : вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576

58. Функції захисту персональних даних покладено на уповноваженого. Уповноважений Верховної Ради України з прав людини : вебсайт. URL: http://www.ombudsman.gov.ua/ua/page/zpd/ (дата звернення: 15.10.2024).

59. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка. 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514

60. Юдін О. К. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів. Наукоємні технології. 2014. № 4(24). С. 462–467.