МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН ТА СТРАТЕГІЧНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувачка випускової кафедри
_____ Ніна РЖЕВСЬКА
« 07 06 » 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ
СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «КІБЕРЗЛОЧИННІСТЬ У МІЖНАРОДНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ: СВІТОВИЙ ДОСВІД ТА ВІТЧИЗНЯНА ПРАКТИКА»

Виконавець: здобувачка вищої освіти 4 курсу, 409 групи, Ященко Тетяна Василівна

Керівник: ст. викладачка кафедри міжнародних відносин та стратегічних студій Ємець Валентина Олександрівна

Нормоконтролер: _____ Валентина ЄМЕЦЬ

КИЇВ 2024

ЗМІСТ

ВСТУП

Актуальність. У наш час кіберзлочинність набуває все більшого значення як предмет обговорення. Прискорений прогрес інформаційних технологій та інтеграція інформаційної сфери в глобальному масштабі визначають цю проблему не тільки як локальну, а й як міжнародну. Кіберзлочинність не знає меж, тому вимагає дій усього людства, об'єднавшись проти неї.

Сьогодні кіберпростір є обов'язковим у житті світу, і зараз важко уявити, що можна було б обійтися без нього, оскільки він проник у всі сфери життя – від економіки до повсякденного спілкування. Це робить його не лише зручним інструментом, а й ареною у війні, в якій Україна, на жаль, слабка. Державні та недержавні економічні процеси стають все більш залежними від кіберпростору. З одного боку, це створює більше можливостей, але з іншого – економіка стає вразливішою до кібератак.

Ця проблема кіберзлочинності, що швидко розвивається, виходить за межі географічних кордонів і постійно змінюється. Поява інформаційних технологій породила безліч нових типів кіберзлочинів, які також необхідно постійно вивчати, щоб розробити ефективні заходи протидії.

Жодна країна не може самостійно вирішити проблему кіберзлочинності. Необхідно об'єднувати зусилля на міжнародному рівні та ділитися досвідом боротьби у цій сфері.

Війна Росії проти України демонструє нову форму агресії, адже кіберзагрози стають ще одним фронтом, на якому відбуваються бойові дії, тобто небезпека виникає навіть у віртуальному світі.

Крім того, слід зазначити, що в боротьбі зі злочинністю в кіберпросторі просто скопіювати досвід інших країн не є ефективним способом. Україні необхідно локалізувати та адаптувати іноземну практику до місцевого середовища та умов. Тут важливо те, що Україна має вжити заходів для

підвищення рівня кібербезпеки держави, адже від цього, крім економічної стабільності, залежить і національна безпека.

Метою дослідження є вивчення впливу кіберзлочинності на міжнародний та вітчизняний інформаційний простір.

Для досягнення поставленої мети необхідно вирішити наступні **завдання:**

– дослідити зміст та особливості інформаційного простору світу та України;

– охарактеризувати поняття, особливості та класифікацію кіберзлочинності;

– проаналізувати досвід протидії кіберзлочинності в інформаційному просторі США, Франції та Німеччини;

– визначити основні загрози безпеці інформаційного простору України;

– розробити рекомендації щодо боротьби з кіберзлочинністю в Україні.

Об'єктом дослідження є кіберзлочинність у міжнародному інформаційному просторі.

Предметом дослідження – особливості реалізації державної політики щодо протидії кіберзлочинності в інформаційному просторі.

Методи дослідження. У роботі використано загальнонаукові методи, Ivent-аналіз для дослідження динаміки кіберзлочинності в Україні під час повномасштабної агресії Росії та SWOT-аналіз для оцінки сильних і слабких сторін, а також можливостей і загроз кібербезпеки України.

Апробація отриманих результатів. Зміст і результати дослідження презентовано на конференціях: «Дипломатія в міжнародних відносинах: сучасні виклики та перспективи» (29 лютого 2024 р., м. Київ), та «Політ. Сучасні проблеми науки» (2-5 квітня 2024 р., м. Київ) [99],[95].

Структура та обсяг. Робота включає в себе вступ, три розділи, висновки та список використаних інформаційних джерел. Загальний обсяг роботи становить 87 сторінок, основний текст викладено на 66 сторінок. Список використаних інформаційних джерел нараховує 100 позицій.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – Інформаційні технології

ІКТ – Інформаційно-комунікаційні технології

НІП – Національний інформаційний простір

РНБО – Рада національної безпеки і оборони України

ЄС – Європейський Союз

ОБСЄ – Організація з безпеки і співробітництва в Європі

ОЗС НАТО – Об’єднані збройні сили НАТО

SHAPE – Supreme Headquarters Allied Command Europe (Верховний штаб Об'єднаних збройних сил НАТО в Європі)

ENISA – The European Union Agency for Cybersecurity (Європейське агентство з мережевої та інформаційної безпеки)

CERT – Команда реагування на комп'ютерні надзвичайні події України

ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information (Французьке Національне агентство з безпеки інформаційних систем)

РОЗДІЛ І.
ТЕОРЕТКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВИ

1.1 Інформаційний простір держави: поняття, особливості, структура

У XXI столітті інформація стає ключовим фактором могутності держави. Володіння найсучаснішими інформаційними технологіями та засобами для обробки, зберігання, передачі та поширення інформації дає державі значні переваги в економічній, військовій, управлінській та соціальній сферах.

Використання інформаційних технологій ефективно сприяє економічному зростанню, покращує конкурентоспроможність бізнесу та допомагає створенню нових робочих місць. Сучасна світова арена ІТ використовується для розвитку, комунікацій та керування в армії, що надає державам переваги у сфері оборони. Ця технологічна ера допомагає урядам ефективніше керувати країною, полегшувати життя громадянам і боротися з корупцією. Крім цього, доступ до цих технологій сприяє покращенню освіти, охорони здоров'я та інших необхідних послуг для людей. Таким чином, належне володарювання сучасною ІТ є ключовим аспектом успішного розвитку будь-якої держави у сучасних умовах [1].

Інформаційний простір існував задовго до появи людини. Фактично, його вік дорівнює віку самої планети Земля, адже навіть неживі елементи природи були і є джерелами різноманітної інформації. Єдина відмінність полягала в тому, що в ті часи не було істот, здатних сприймати, запам'ятовувати, обробляти та використовувати цю інформацію. Із зародженням життя, навіть на найпростіших його рівнях, інформаційний простір почав наповнюватися змістом, набувати сенсу та усвідомлюватися живими організмами. Поступово, зі складним розвитком різноманітних форм життя на Землі, одночасно розвивався і ставав багатшим інформаційний простір, який їх оточував [2].

З одного боку, інформаційний простір можна розглядати як сукупність інформаційних ресурсів, доступних людям та організаціям. Ці ресурси включають тексти, зображення, аудіо та відео записи, бази даних, а також інші форми інформації. З іншого боку, інформаційний простір також можна розуміти як середовище, в якому відбувається обмін інформацією. Це середовище включає в себе не лише інформаційні ресурси, але й канали зв'язку, технології та інструменти, які використовуються для обміну інформацією.

Згідно з висловлюванням Калюжного Р., інформаційний простір можна розділити на три сфери:

– сфера єдиного інформаційного простору країни, що охоплює внутрішній інформаційний обмін та комунікацію всередині країни;

– сфера інформаційної взаємодії країни з іншими державами, тобто обмін інформацією та здійснення комунікації на міжнародному рівні між країнами;

– сфера інформаційного простору, яка має особливе значення для вирішення конкретних проблем в економічній, політичній і культурній сферах у контексті міжнародного співробітництва. Ця сфера стосується обміну інформацією та здійснення комунікації, що необхідні для ефективної взаємодії та вирішення питань у процесі міжнародної співпраці в різних галузях [3].

Важливо розуміти, що інформаційний простір не статичний. Він постійно змінюється та розвивається, завдяки появі нових інформаційних ресурсів, технологій та інструментів. Ці зміни мають значний вплив на те, як люди та організації отримують, обробляють та використовують інформацію [4].

У контексті інформаційного простору держави ці зміни мають ще більшу вагу. З одного боку, вони відкривають нові можливості для доступу до інформації, участі в суспільному житті та розвитку демократії. З іншого боку, вони також створюють нові виклики, такі як поширення дезінформації, пропаганди та кіберзлочинності. На сьогоднішній день існує безліч визначень інформаційного простору держави.

Інформаційний простір та пов'язані з ним явища привертали увагу багатьох видатних науковців з різних дисциплін. Наприклад, Тім Бернерс-Лі,

британський вчений, заклав основи сучасного інформаційного простору Інтернету, винайшовши Всесвітню павутину [5]. Але дослідження інформаційного простору не обмежується сферою інформаційних технологій. Науковці з різних галузей знань зробили значний внесок у розуміння цієї складної концепції. Так, у сфері інформатики Грегорі Ньюбі та Джейсон Візроу досліджували технічні аспекти інформаційного простору, його структуру, функціонування та можливості. Філософський дискурс про інформаційні простори можна знайти в працях Норберта Вінера та Марини Яковенко [6].

Інформаційний простір держави – це сукупність численних текстових, аудіо- та відеоповідомлень, оприлюднених або запланованих до оприлюднення на її території; динамічне середовище, яке включає у себе безліч інформаційних ресурсі, таких як тексти, зображення, аудіо та відео записи, бази даних та інші форми інформації [8].

Український дослідник Михайло Слюсаревський обґрунтовує реляційну теорію інформаційного простору. Згідно з його концепцією, інформаційний простір є станом і водночас результатом постійної взаємодії процесів створення та споживання інформації. Дослідник вважає, що самі по собі процеси виробництва інформації не можуть надати інформаційному простору чіткого визначення та просторових меж. Ці просторові параметри формуються лише через процеси споживання інформації. На думку вченого, характеристики інформаційного простору зумовлені темпорально-психологічними (пов’язаними з часом та психологією) особливостями перебігу інформаційних процесів, а також соціально-психологічними характеристиками споживачів інформації. Тому в рамках реляційної теорії М.Слюсаревський пропонує характеризувати цю категорію не стільки за обсягами виробництва інформаційної продукції чи площею поширення інформації, скільки за обсягами та інтенсивністю її споживання [7].

Існує два типи інформаційного простору держави: внутрішній та зовнішній. Той простір, що обмежується кордоном держави називають

внутрішнім. Території певних держав, де визначена держава має свої окремі інтереси (військові, фінансові тощо) – зовнішнім [8].

Будучи основою політичного, соціально-економічного та культурного розвитку забезпечення безпеки держави, інформаційний простір держави складається з таких основних компонентів як:

– Інформаційні ресурси, а саме: збірки інформації, доступ до яких отримують за допомогою спеціального програмного забезпечення; усі види архівів; системи депозитаріїв державних інформаційних ресурсів; збірки книг, журналів та інших друкованих матеріалів.

– Система інформаційно-комп'ютерних технологій, що охоплює базові, прикладні й забезпечувальні компоненти.

– Структури організації, включаючи кадровий потенціал, необхідні для функціонування та прогресу національної інформаційної інфраструктури.

– Сегмент ринку, що охоплює інформаційні технології, засоби зв'язку, інформатизацію та телекомунікації, а також вироби й послуги у цій галузі.

– Система масової інформації.

– Система забезпечення та підтримання інформаційного захисту.

– Інформаційне законодавство.

– Цифрові платформи.

– Державна інформація, що включає у себе дані та інформацію, надана різними державними установами та відомствами [9].

Одним з ключових факторів забезпечення національних інтересів, формування громадської думки та реалізації державної політики в умовах сучасного інформаційного суспільства є створення та розвиток ефективного національного інформаційного простору. Цей феномен має низку специфічних рис та особливостей, що відображають роль держави у регулюванні інформаційних потоків, забезпеченні інформаційної безпеки та незалежності, а також визначають його стратегічну значущість для розвитку суспільства та держави загалом.

Якщо розглядати особливості інформаційної сфери держави, то тут можна виокремити саме відкритість та доступність. З одного боку, для досягнення максимальної ефективності інформаційний простір має бути відкритим для всього суспільства. Така відкритість дозволить гармонійно поєднати та реалізувати інтереси громадян, суспільних груп та держави на засадах комплексності й системності [10]. Але з іншого боку, критично важливі інформаційні ресурси, дані та системи повинні надійно захищатися від несанкціонованого доступу й витоку відомостей з міркувань національної безпеки.

Технологічний розвиток також є одним з особливостей інформаційного простору, адже його ефективне функціонування в сучасних умовах неможливе без розбудови відповідної технологічної інфраструктури. Державам необхідно постійно та активно розвивати та модернізувати телекомунікаційні мережі, системи передачі даних, цифрові платформи, впроваджувати новітні ІКТ [11]. Адже це, в свою чергу, забезпечує якісний доступ громадян до інформаційних ресурсів, підвищує рівень медіаграмотності та цифрових компетенцій населення. Важливим є й розвиток вітчизняної ІТ-індустрії для створення національного контенту та програмного забезпечення.

Забезпечення інформаційного суверенітету та безпеки – є головною характеристикою інформаційного простору держави. Держава повинна мати суверенітет над своїм національним інформаційним простором, що означає контроль над його формуванням, регулюванням та захистом. Це необхідно для того, щоб не допустити будь-якого неправомірного втручання ззовні, що може завдати масштабної шкоди інформаційним ресурсам, критичній інфраструктурі та національним інтересам країни. Забезпечення інформаційного суверенітету є невід’ємною складовою державного суверенітету в цілому та має вирішальне значення для збереження національної безпеки, територіальної цілісності та незалежності [12].

Тому, держава зобов’язана вживати сурових заходів безпеки для надійного захисту свого інформаційного простору від широкого спектру

зовнішніх загроз, а саме кібератак, поширення шкідливого і незаконного контенту, цілеспрямованої дезінформації, деструктивної пропаганди та інформаційних операцій. Необхідним є також безперервний моніторинг інформаційних потоків, аналіз ризиків та своєчасне реагування на виклики. Велика увага має приділятися протидії інформаційним операціям та гібридним загрозам, що можуть цілеспрямовано застосовуватися для дестабілізації внутрішньої суспільно-політичної ситуації, підриву суспільної довіри, маніпулювання суспільною свідомістю та просування ворожих наративів.

Розглядаючи, суверенітет та безпеку, як ключову особливість інформаційного простору, потрібно знайти баланс та не ігнорувати дотримання основоположних прав та свобод громадян своєї держави. Громадянам повинно бути гарантовано вільний доступ до інформації, особливо у мережі Інтернет, свободу слова, незалежність медіа та безперешкодний обмін ідеями й думками. А за умови розумного балансу між інформаційною безпекою та демократичними свободами можна досягти сталого розвитку національного інформаційного простору.

Проте, незважаючи на пріоритет у забезпеченні інформаційного суверенітету, жодна держава на сьогоднішній день не може повністю дистанціюватися від глобальних інформаційних потоків, процесів та викликів. Інформаційний простір є надзвичайно динамічним середовищем, на яке впливають численні зовнішні чинники. Тому, для ефективного захисту та розвитку власного безпечного інформаційного простору важливою є активна участь країни у міжнародній інформаційній взаємодії та співпраці на різних рівнях.

Належним чином протистояти глобальним загрозам, можна шляхом тісної співпраці між державами, обміном досвідом, міжнародним організаціям. Саме співпраця між країнами, яка, у свою чергу, підвищує ефективність розробки спільних програм для боротьби з кіберзлочинністю, відстежування та блокування шкідливого контенту, виявлення та припинення поширення

операцій ворожих акторів, відкриває можливості для розробки спільних підходів до регулювання в інформаційній сфері.

1.2 Безпека інформаційного простору України

В епоху стрімкого розвитку інформаційно-комунікаційних технологій та зростаючої ролі інформаційного простору в усіх сферах життєдіяльності суспільства, питання захисту національних інтересів набуває неабиякої важливості. Інформаційний простір став одним із визначальних факторів забезпечення національної безпеки держави, оскільки він охоплює інформаційні ресурси, інфраструктуру, суб'єктів та системи формування національних інформаційних ресурсів.

Враховуючи зростаючі загрози, кібератаки, поширення деструктивного контенту, витоку даних та порушень прав інтелектуальної власності, забезпечення безпеки інформаційного простору України є нагальною потребою сучасності. Злочини у кіберпросторі несуть серйозні ризики для держави, бізнесу та громадян, завдаючи значних економічних та іміджевих втрат.

Національний інформаційний простір України – це динамічна система, що постійно розвивається, й на яку впливають різноманітні фактори. За роки незалежності України НІП зазнав значних змін, пройшовши шлях від радянської цензури до інформаційної відкритості та свободи слова.

Саме створення національної інформаційної сфери України почалось наприкінці 80-х – початку 90-х рр. XX ст., та поділяється на три етапи. Перший етап бере свій початок з 1989 р. по 1990 р. Протягом цих років почали виникати громадські та молодіжні об'єднання, політичні партії та рухи. Це призвело до появи понад 1200 неформальних друкованих видань, які не проходили цензуру радянської влади [13].

Другий етап (1990-1991 р.р.) розпочався після прийняття Закону СРСР «Про пресу та інші засоби масової інформації». Цей закон легалізував незалежні ЗМІ і сприяв їх бурхливому розвитку. За цей період було

зареєстровано понад 2,5 тис. центральних, регіональних та місцевих друкованих видань [14].

З 1991 р. по 1992 р. був третій етап пов'язаний із здобуттям Україною незалежності. Відбулася департизація державних органів, установ та організацій, а також перереєстрація періодичних друкованих видань. Засновниками багатьох з них перестали бути центральні, регіональні та місцеві органи Комуністичної партії України [15].

Розвиток незалежних демократичних ЗМІ став одним із найважливіших досягнень періоду становлення НІП. Незалежні видання відігравали важливу роль у формуванні громадянського суспільства та демократії в Україні. Для їх розвитку були закладені законодавчі основи, а саме закони «Про інформацію» та «Про друковані засоби масової інформації (пресу) в Україні», що гарантували право на свободу слова, також завдяки цим законам приватним особам відкрили можливість бути засновниками медіа [16, с.73].

Прийняття Постанови Верховної Ради України «Про департизацію державних органів, установ та організацій» та Указу Президії Верховної Ради України «Про заборону діяльності Комуністичної партії України (КПУ)» у серпні 1991 р. відкрило нові горизонти для розвитку українських медіа. Ці важливі рішення сприяли демонополізації інформаційного простору та створили сприятливі умови для появи значної кількості нових видань [17]. Наприкінці 1991 р. чисельність загальнонаціональних газет, що були зареєстровані зросла з 19 до 290, а 180 журналів стали новими виданнями з 262 загальнонаціональних зареєстрованих. Такий стрімкий розвиток медіа став свідченням демократичних перетворень та свободи слова в незалежній Україні [18, с.6].

У період з 1994 р. по 2004 р. відбувалася структуризація національного інформаційного простору України. На цьому етапі визначалися ключові гравці медіаринку та формувалися лідери серед них. Створювалася система координації діяльності учасників інформаційної сфери, а також окреслювалися пріоритети подальшого розвитку та інтеграції до європейського й світового

інформаційних просторів. Державні органи, такі як Міністерство у справах преси та інформації, Державний комітет телебачення і радіомовлення України, Міністерство інформації України, а також колегіальний орган – Національна рада з питань телебачення і радіомовлення, брали на себе відповідальність за становлення інформаційного простору України, його розвиток у правовому полі та забезпечення безпеки [19].

У період 2005-2014 рр. Україна розробляла нову інформаційну політику, враховуючи вимоги глобального інформаційного середовища, потенційні загрози та необхідність забезпечення інформаційної безпеки. Орієнтація на європейські стандарти визначала стратегію розвитку. У цій новій політиці були визначені ряд стратегічних напрямків, включаючи постійне удосконалення Концепції національної інформаційної політики, реалізацію Програми інформатизації, впровадження системного Інформаційного кодексу, створення Національного фонду цифрової культурної спадщини, та розвиток безперервного національного інформаційного простору [20].

Також, були проведені заходи з підвищення освітньої свідомості за допомогою інформаційно-комунікаційних технологій, а також об’єднання громадських організацій в Асоціацію громадських сил з метою захисту свободи слова та незалежності ЗМІ. Але попри це, у 2008 р. інформаційний простір України відчув наслідки світової фінансової кризи. Багато редакцій були змушені скоротити штат працівників та зменшити їхню заробітну плату внаслідок зниження обсягів рекламних витрат [21, с. 162].

Початок масових протестів в Україні, відомих як «Євромайдан» і «Революція гідності» у листопаді 2013 р., різко висвітлив усі прорахунки в інформаційній сфері країни за попередні роки. У цей період Росія застосовувала агресивну інформаційну політику, що призвело до викривлення та спотворення іміджу України в усьому світі, особливо в самій Росії. Лише завдяки активному висвітленню цих подій провідними європейськими та світовими медіа, такими як Thomson-Reuters, AFP, AP, TVP, CNN, BBC, Al'Jazira та інші, вдалося порушити багаторічну традицію отримання інформації

про Україну лише з російських джерел. Однак ця обставина ще раз підкреслила, наскільки важливим є для України створення власної системи постачання інформації у світовий інформаційний простір, а також розробки ефективних механізмів протидії інформаційній агресії.

На початку 2014 р. на території Автономної Республіки Крим, окрім присутності військового контингенту Російської Федерації, здійснювався інформаційно-психологічний тиск на населення України з боку ЗМІ іноземної держави. Спостерігалася інформаційна експансія в національний інформаційний простір України, а також захоплення стратегічних об'єктів української телекомунікаційної інфраструктури. Ці дії відбувалися на тлі масованого й агресивного інформаційного наступу російської пропаганди, яка, всупереч європейським стандартам у сфері медіа, намагалася розпалювати в Україні, зокрема в Криму, міжнаціональну ворожнечу та сепаратистські настрої, посягаючи на державний суверенітет і територіальну цілісність України [22].

Для виправлення прорахунків у вітчизняній інформаційній політиці, Україною було реалізовано такі інформаційні проєкти, а саме за рішенням Ради національної безпеки і оборони було припинено трансляцію російських телеканалів «Россия 24», ОРТ (Первый канал всемирная сеть), «РТР Планета», «НТВ-Мир». Крім того, було запроваджено суспільне телебачення і радіомовлення, встановлено нагляд за дотриманням медіа виборчого законодавства, а також створено Міністерство інформаційної політики [23]. Ці заходи мали на меті протидіяти інформаційній агресії, забезпечити об'єктивне висвітлення подій та зміцнити інформаційний суверенітет держави.

Інформаційний простір є критично важливим для національної безпеки та розвитку будь-якої держави в сучасному світі. Адже, безпека інформаційного простору передбачає збереження інформаційного суверенітету держави шляхом захисту від інформаційних загроз, спрямованих на підрив національної ідентичності, цінностей, незалежного прийняття рішень та сталого розвитку суспільства і держави в стратегічних сферах життєдіяльності [24].

Сучасні суспільно-політичні умови існування України та геополітичні фактори, на той момент, спричинили нагальну потребу посилити заходи інформаційної безпеки держави, зокрема створити Доктрину та Концепцію інформаційної безпеки України. Цю функцію взяло на себе Міністерство інформаційної політики [25]. Позитивним моментом цих документів стало нормативне визначення низки термінів, пов'язаних зі стратегічними комунікаціями. Разом з тим, правозахисників непокоїла можливість блокування та видалення ворожих інтернет-ресурсів, закладена в Доктрині. Дискусійним був також визначений нею підхід до реалізації з залученням численних державних органів.

Сприятливим кроком для інформаційної безпеки стало припинення ретрансляції 86 російських програм відповідно до законодавства та міжнародних норм. Це зменшило пропагандистські потоки та сприяло появі нових українських супутникових каналів.

Водночас серйозними викликами залишилися фінансові та організаційні проблеми Суспільного мовлення, перешкоджання журналістській діяльності, порушення під час висвітлення виборів, зокрема поширення фейків та пропаганди. Ці фактори гальмували демократичний розвиток інфопростору та негативно позначалися на іміджі України.

Національний інформаційний простір є могутнім інструментом зміцнення держави та формування нації, що відіграє ключову роль у забезпеченні національної безпеки кожної країни. Відомий політолог Збігнєв Бжезінський висловив думку, що у соціально-економічному аспекті світ перетворюється на єдине поле гри, де дедалі більшого значення набувають три динамічні реалії: глобалізація, «інтернетизація» та дерегулювання». Процес інтернетизації або глобальний вплив на інформаційний простір визначають могутність та вплив сучасних держав. Іншими словами, здатність ефективно використовувати і контролювати інформаційні потоки та інтернет-простір є одним з ключових чинників, що формують силу і авторитет країн у наш час [26].

Стратегічною метою української інформаційної політики стало забезпечення переходу України до інформаційного суспільства та входження до світового цивілізаційного розвитку. Ефективне керування інформаційними ресурсами, інфраструктурою та державна підтримка інформаційного виробництва, ринку інформаційних технологій, продуктів і послуг – це ключові аспекти успіху.

На жаль, перед національним інформаційним простором України й на сьогодні постають серйозні загрози та виклики, що несуть небезпеку для функціонування держави, її політичного та економічного розвитку, а також процесу інтеграції України до європейських та євроатлантичних структур.

Загрози національній безпеці України в інформаційній сфері – це сукупність обставин і факторів, які створюють ризики для життєво важливих інтересів держави, суспільства і громадян через можливість негативного впливу інформації на свідомість та поведінку людей, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру країни. Іншими словами, це умови, за яких інформаційний вплив може завдати шкоди громадянам, спричинити деструктивні наслідки для інформаційних систем і загалом підірвати інформаційну безпеку держави [27].

У Законі України «Про основи національної безпеки» зазначено, що одна з головних небезпек для інформаційної сфери – це спроби маніпулювати суспільною свідомістю, шляхом розповсюдження недостовірної, неповної або упередженої інформації [28].

У Доктрині інформаційної безпеки України описано головні виклики для забезпечення інформаційної безпеки країни:

– поширення у глобальному інформаційному просторі перекрученої, недостовірної та упередженої інформації, яка завдає шкоди національним інтересам України;

– зовнішні деструктивні впливи на суспільну свідомість через засоби масової інформації та Інтернет;

– руйнівні інформаційні впливи, що спрямовані на саботаж конституційного ладу, суверенітету, територіальної цілісності та недоторканності держави;

– прояви сепаратизму у медіа та Інтернеті за етнічною, мовною, релігійною та іншими ознаками [29].

На думку Р.Марятян, загрозою національної безпеки України в інформаційному просторі є цілеспрямовані інформаційні заходи з боку інших країн, метою яких є формування в українців та міжнародної спільноти вигідного для них світогляду та уявлень шляхом маніпулятивного впливу на масову свідомість. Така загроза реалізується шляхом систематичного поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її території. Це негативно впливає на зовнішню та внутрішню політику нашої держави, підриває її міжнародний імідж і має політичні та економічні підстави. Метою таких цілеспрямованих інформаційних операцій є забезпечення національних інтересів інших держав за рахунок України. Іншими словами, відбувається цілеспрямована дезінформаційна кампанія щодо України через поширення викривленої чи неповної інформації для формування вигідного певним країнам уявлення про ситуацію в нашій державі. Це дозволяє їм реалізовувати свої національні інтереси, завдаючи шкоди іміджу, політиці та економіці України [30].

До загроз національній безпеці держави в інформаційній сфері науковці також відносять:

– обмеження свободи слова та можливостей громадян отримувати інформацію;

– викривлення, зміщення, обмеження, маскування або однобічне подання інформації;

– несанкціоноване поширення інформації, відкрита дезінформація;

– інформаційна експансія з боку інших держав та руйнівне інформаційне вторгнення у вітчизняний інфопростір, коли країни з

потужнішими інфоресурсами розширюють свій вплив через ЗМІ на населення України;

– виникнення і функціонування в національному інформпросторі некерованих інформаційних потоків;

– поширення у ЗМІ культу насильства, жорстокості;

– повільна інтеграція України до світового інформаційного простору;

– невиважена державна інформаційна політика та відсутність необхідної інфраструктури;

– розміщення дезінформації в Інтернеті.

Слід відзначити, що для захисту національного інформаційного простору та забезпечення ефективної інформаційної безпеки українська влада приймала та продовжує приймає ряд заходів. Наприклад, 14 січня 2015 року Кабінет Міністрів України затвердив Постанову, відповідно до якої було створено Міністерство інформаційної політики України. Основними завданнями цього відомства є протидія інформаційній агресії з боку Російської Федерації, розроблення ефективної стратегії інформаційної політики країни та Концепції інформаційної безпеки України, а також забезпечення узгодженості та координації роботи органів державної влади у сфері інформації [31].

Рада національної безпеки і оборони України прийняла рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», щоб протистояти негативним наслідкам інформаційної пропаганди та інформаційних війн, а також запобігати та нейтралізувати реальні та потенційні загрози в інформаційному просторі України.

У цьому документі йдеться про те, що РНБО, враховуючи потребу в поліпшенні нормативно-правового забезпечення та запобіганні й нейтралізації можливих загроз національній безпеці в інформаційній сфері, прийняла рішення:

– Посилити контроль за виконанням законодавства у сфері інформаційно-психологічної та кібернетичної безпеки.

– Розробити та внести на розгляд Верховної Ради України законопроекти, що передбачають зміни до деяких законів України, спрямовані на протидію інформаційній агресії з боку іноземних держав. Ці зміни передбачають встановлення механізму протидії негативному інформаційно-психологічному впливу, у тому числі заборону ретрансляції телевізійних каналів.

– Здійснити заходи для поширення об'єктивної інформації про суспільно-політичну ситуацію в Україні на міжнародному рівні, зокрема, шляхом створення відповідного медіахолдингу для створення якісного та конкурентоспроможного інформаційного продукту.

– Розробити методику аналізу інформаційних матеріалів іноземних ЗМІ для встановлення ефективного механізму акредитації журналістів.

– Здійснити заходи для зміцнення міжнародного співробітництва в питаннях протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності [32].

Окрім вищезгаданого рішення РНБО, основні напрямки державної політики з питань національної безпеки в інформаційній сфері визначені в наступних документах:

– Закон України «Про основи національної безпеки України» [61].

– Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [62].

– Доктрина національної безпеки України [63].

– Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року [64].

– Доктрина інформаційної безпеки України, затверджена Указом Президента України від 29 грудня 2016 року [65].

– Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 4 березня 2016 року [66].

– Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року [67].

– Указ Президента «Про рішення Ради національної безпеки і оборони України» від 14 травня 2021 року «Про Стратегію кібербезпеки України» [68].

Ці документи визначають такі пріоритетні завдання:

– захист інформаційного суверенітету України;

– протидія інформаційним загрозам, зокрема дезінформації та пропаганді;

– розвиток національної інформаційної інфраструктури;

– підвищення кібербезпеки;

– забезпечення інформаційної грамотності населення.

Реалізація цих завдань має на меті забезпечити стійкість України до інформаційних атак та зберегти національну безпеку в інформаційній сфері.

З початком повномасштабної агресії Росії кіберпростір України зазнав активних атак. Для протидії їм та забезпечення кібербезпеки країни в умовах воєнного стану були задіяні спеціальні структури. Зокрема, при Службі безпеки України почав функціонувати Ситуаційний центр забезпечення кібербезпеки, обладнаний системою керування інформаційними подіями. Ця система дозволяє відстежувати кіберінциденти в режимі реального часу, аналізувати стан інформаційної безпеки держави, оперативно виявляти та протидіяти різноманітним кіберзагрозам в українському сегменті кіберпростору. А на базі кіберполіції були сформовані спеціалізовані підрозділи, відповідальні за виявлення, аналіз та нейтралізацію випадків дезінформації, зокрема, матеріалів із використанням технологій діпфейків [33].

Для фінансового забезпечення невідкладних заходів із захисту інформаційної сфери в умовах російської агресії у 2022 році було видано Розпорядження КМУ №366-р «Про виділення коштів з резервного фонду державного бюджету щодо забезпечення інформаційної безпеки та захисту інформаційного простору держави». Цим документом з резервного фонду державного бюджету були виділені кошти на реалізацію комплексної програми із зміцнення інформаційної безпеки України. Зокрема, виділене фінансування передбачалося спрямувати на створення мережі ситуаційних центрів для

моніторингу та реагування на інформаційні загрози, закупівлю спеціалізованого програмного забезпечення для виявлення і нейтралізації ворожої пропаганди, фейків, підвищення рівня кібербезпеки критичної інфраструктури. Окремі асигнування були виділені на проведення широкої інформаційної кампанії для підвищення медіаграмотності громадян і формування стійкості до деструктивного інформаційно-психологічного впливу з боку Росії [34]. Окрім цього для комплексного реагування на виклики в інформаційній сфері в умовах воєнної агресії РФ Постановою Кабінету Міністрів №276 від 8 березня 2024 р. була утворена Міжвідомча робоча група з питань отримання закордонної підтримки для забезпечення кібербезпеки та кіберстійкості держави. До складу групи увійшли представники профільних міністерств, відомств, Ради національної безпеки і оборони та Служби безпеки України.

Основними завданнями робочої групи є визначення потреб у міжнародній технічній, консультаційній, фінансовій та іншій допомозі в галузі кібербезпеки, налагодження взаємодії з іноземними партнерами, координація процесів отримання такої допомоги.

Діяльність групи спрямована на посилення співпраці з союзниками для підвищення можливостей України протидіяти ворожим кібератакам, убезпечення критичної інформаційної інфраструктури, а також розбудови стійкої системи кібербезпеки відповідно до найкращих міжнародних стандартів і практик [35].

РОЗДІЛ ІІ.
КІБЕРЗЛОЧИНИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

2.1. Основні поняття та класифікація кіберзлочинності

Ера цифрових технологій відкрила нові горизонти можливостей для людства, але водночас спричинила появу нових загроз та викликів. Стрімкий розвиток Інтернету, поширення смартфонів, зростання популярності соціальних мереж та хмарних технологій започаткували нову еру злочинності, яка не знає кордонів – кіберзлочинність.

Незважаючи на відсутність чітко встановленої історії кіберзлочинів, більшість експертів виділяють певну подію як перший задокументований випадок хакерської атаки. За технічними стандартами, першою зафіксованою кібератакою вважається інцидент, що стався у Франції в 1834 р., задовго до появи Інтернету. Зловмисники зламали французьку телеграфну мережу та змогли викрасти конфіденційні дані фінансового ринку. З цього моменту відбувся стрімкий сплеск кіберзлочинності, який супроводжувався захопливою еволюцією стратегій та методів, що використовуються злочинцями для досягнення своїх протиправних цілей. Кіберзлочинність невпинно розвивалася, адаптуючись до нових технологій та знаходячи нові способи вчинення правопорушень [36].

Зараз же кіберзлочинність набула дійсно масштабних розмірів і стала серйозною проблемою для звичайних людей, бізнесу та національних інтересів різних країн. Зі стрімким розвитком цифрових пристроїв та сервісів, від яких залежить функціонування людства, злочинці отримали величезні можливості для протиправних дій. Хакери надзвичайно креативні, постійно вдосконалюють свої методи та знаходять нові, більш витончені способи обходу систем безпеки. Вони швидко адаптуються до новітніх тенденцій, таких як хмарні сервіси або штучний інтелект, використовуючи їх як потенційні шляхи для кібератак. Крім того, злочинні групи стають все більш організованими і професійними,

пропонуючи кіберзлочинність як послугу з чітким розподілом ролей і спеціалізацією. Це постійне технологічне протистояння між кіберзлочинцями і фахівцями з кібербезпеки вимагає технологічного розвитку, інновацій та міжнародного співробітництва для захисту критично важливих систем і даних.

Загалом, у широкому розумінні кіберзлочинність – це будь-яка незаконна діяльність, що відбувається в Інтернеті або через комп'ютерні системи [69].

Дебараті Халдер і К. Джайшанкар визначають кіберзлочинність як правопорушення, скоєні проти окремих осіб або груп зі злочинним наміром, для навмисного знищення репутації жертви або завдання фізичної, моральної або фінансової шкоди, прямо чи опосередковано, використовуючи сучасні телекомунікаційні мережі, такі як Інтернет (чати, електронна пошта, дошки оголошень і групи) і мобільні телефони (SMS/MMS) [37].

За визначенням Оксфордського словника термін кіберзлочинність відноситься до злочинних дій, що здійснюються з використанням комп'ютерних технологій або Інтернету [38]. Ці злочини можна розділити на дві категорії: злочини, в яких комп'ютер використовується як інструмент для полегшення незаконної діяльності (наприклад, шахрайство або хакерство), і злочини, в яких сам комп'ютер є мішенню (наприклад, віруси або відмова в обслуговуванні, атаки) [39].

У книзі «Індійське кіберзаконодавство з кіберглосарієм» професор С.Т. Вішванатан надає три визначення терміну кіберзлочинність:

1. Будь-яке протиправне діяння, в якому комп'ютер є знаряддям, тобто будь-який злочин, засобом або метою якого є вплив на роботу комп'ютера.

2. Будь-який інцидент, пов'язаний з комп'ютером, в якому жертва зазнала або могла зазнати шкоди, а злочинець, за наміром, отримав або міг отримати вигоду.

3. Будь-яка незаконна, неправомірна або несанкціонована діяльність, пов'язана з автоматичною обробкою та передачею чужих даних [40].

Основною ознакою кіберзлочинності виступає той факт, що кіберзлочини вчиняються у межах віртуального простору або комп'ютерних мереж.

Віртуальний простір – це інформаційний простір, що модульований за допомогою комп'ютерів, який містить дані про людей, факти, явища та процеси, представлені в математичній, символічній чи іншій формах [41].

Наступною ознакою кіберзлочинності можна назвати те, що самим кіберзлочиннам притаманний інтелектуальний характер, оскільки здійснення кіберзлочинів потребує певного рівня знань та навичок. Окрім того, субкультура хакерів пропагує ідею інтелектуального саморозвитку, що слугує додатковим стимулом для кіберзлочинців.

Додатковим показником ознаки кіберзлочинності виступають анонімність та безособовість. На відміну від традиційних злочинів, де злочинець і жертва часто знаходяться поруч, у кіберпросторі відстань між ними може сягати тисяч кілометрів. Кіберзлочинці можуть ретельно приховувати свою справжню особистість, використовуючи підроблені дані, технології анонімізації та інші методи маскування. Це дозволяє їм уникати відстеження і залишатися невідомими для правоохоронних органів. Анонімність також посилює відчуття безкарності та знижує психологічний бар'єр для вчинення протиправних дій. Жертви кіберзлочинів часто навіть не знають, хто стоїть за атакою. Кіберзлочинець та його жертва можуть перебувати на величезній відстані одне від одного, що робить ці правопорушення віддаленими [70].

Ці особливості є основою для дослідження класифікацій кіберзлочинів та факторів, що впливають на них у сучасному інформаційному середовищі.

На даний момент у світі існує багато видів кіберзлочинності – від простих атак до складних, масштабних кібератак на великі організації та державні установи. Ця тенденція з часом лише посилюватиметься, оскільки доступність технологій, які можуть бути використані для вчинення кіберзлочинів, зростає, а методи захисту вдосконалюються, що змушує злочинців постійно адаптуватися і розробляти нові методи атак. Але серед найпоширеніших видів кіберзлочинів виділяють:

1. Кіберпереслідування: Кіберпереслідування можна визначити як погрозливу поведінку або небажані дії чи переслідування через Інтернет,

електронну пошту, соціальні мережі або текстові повідомлення. Воно має певну схожість з переслідуванням у тому, що є навмисним, наполегливим і особистим і включає в себе стеження, переслідування або контакт з іншими особами в небажаний спосіб. Злочинці можуть переслідувати своїх жертв упродовж тривалого часу, ображати їх у непристойний і зневажливий спосіб або шантажувати секретними фактами. Стежачи за жертвами в Інтернеті, переслідувач отримує інформацію про час, місце і всі необхідні умови для скоєння злочину [42].

2. Кіберзалякування (кібербулінг): форма цькування, яка відбувається за допомогою цифрових пристроїв, таких як мобільні телефони, комп'ютери та планшети. Кіберзалякування може відбуватися через текстові повідомлення, додатки або соціальні мережі, форуми чи ігри, де люди можуть переглядати, брати участь або обмінюватися контентом. Кібербулінг передбачає надсилання, розміщення або обмін негативним, шкідливим, неправдивим або образливим контентом про когось іншого. Це може включати обмін особистою або приватною інформацією про когось, сором чи приниження когось. Деякі види кібербулінгу перетинають межу з незаконною або злочинною поведінкою [43].

3. Фішинг: Термін «фішинг» означає спробу крадіжки конфіденційної інформації, зазвичай у вигляді імен користувачів, паролів, номерів кредитних карток, банківських реквізитів або інших важливих даних, з метою використання або продажу викраденої інформації. Видаючи себе за надійне джерело і роблячи спокусливий запит, хакер заманює жертву в пастку, подібно до того, як рибалка використовує наживку, щоб зловити рибу [44].

4. DDoS-атаки: Атаки спрямовані на те, щоб зробити недоступними онлайн-сервіси та спричинити перебої в роботі мережі, навантажуючи веб-сайт або систему трафіком з різних джерел. Для цього створюються великі мережі заражених комп'ютерів, відомі як ботнети, шляхом вбудовування шкідливого програмного забезпечення в комп'ютери користувачів. Після того, як мережа перестає працювати, хакери отримують контроль над системою [45].

5. Атака Salami: Це вид фінансового шахрайства, який передбачає крадіжку невеликих сум грошей з великої кількості рахунків. Крадіжка невеликих сум грошей із кожного рахунку протягом тривалого періоду часу є метою цього типу атаки, щоб уникнути виявлення. Злодії можуть досягти цього, маніпулюючи фінансовими транзакціями таким чином, щоб їх було важко виявити [46].

6. Атаки вірусами: це особливий тип шкідливого програмного забезпечення, який здатен до самовідтворення та саморозповсюдження. Він проникає у комп'ютерну систему, непомітно підключаючись до інших програм. Зараження вірусом стається відразу після відкриття зараженого файлу, наприклад надісланого електронною поштою. Після того, як вірус потрапляє у систему, він автоматично відтворює себе і поширюється на інші програми та файли. Ці віруси становлять серйозну загрозу, викрадаючи або знищуючи важливі дані та зупиняючи роботу комп'ютерної системи. Зловмисники створюють ці віруси, щоб незаконно викрасти конфіденційну інформацію організації, таку як фінансові дані, бази даних клієнтів і комерційні таємниці. Після викрадення, дані часто використовуються для вимагання викупу від організації-жертви, і цей тип кіберзлочинів стає все більш поширеним [47].

7. Кібертероризм: Це навмисна атака на комп'ютерні системи, програми та бази даних, яка здійснюється з політичних мотивів і загрожує або безпосередньо призводить до актів насильства. Сюди відносяться всі хакерські атаки, спрямовані на залякування населення певної країни. Такі атаки часто намагаються завдати шкоди критично важливим об'єктам інфраструктури, функціонування яких необхідне для нормальної роботи соціальних, економічних, політичних і бізнес-структур. Для здійснення своїх атак кібертерористи використовують звичайні комп'ютери, сервери та мережі, підключені до загальнодоступного Інтернету. Вони часто націлені на захищені урядові мережі та інші системи з обмеженим доступом. Банки, військові об'єкти, електростанції, центри управління повітряним рухом, водоканали тощо також є мішенями [48].

З 2014 року Росія активно здійснює кібератаки проти України, спрямовані на різні сфери, включаючи державні органи, політичних діячів, критичну інфраструктуру та приватний сектор. Масштаби та інтенсивність цих атак лише зростають з плином часу.

Статистика та приклади кібератак свідчать про системний характер загрози. У сфері державного управління та політики мали місце такі інциденти: у 2014-2015 роках було здійснено атаку на український виборчий сервер з метою впливу на результати виборів. У 2017 році відбулася потужна кібератака на Державну казначейську службу і Міністерство фінансів за допомогою вірусу Petya, що паралізувало роботу установ на кілька днів. А впродовж 2022-2023 років уряд та інші державні організації піддавалися безперервним атакам, спрямованим на крадіжку даних та дестабілізацію ситуації в країні.

Критична інфраструктура також зазнала серйозних ударів. У 2015 році відбулася революційна атака на українську енергосистему, що призвела до масового відключення електропостачання у Західній Україні – це була перша у світі успішна кібератака на енергомережу. У 2016 та 2022 роках мали місце додаткові атаки на енергетику та транспорт, з використанням шкідливого ПЗ Industroyer та вторгненням в IT-системи залізниці й аеропортів.

Приватний сектор також постраждав. Масштабна атака вірусу Petya 2017 року завдала величезних збитків не лише державним установам, а й приватним підприємствам, фінансовим організаціям, медіа. А в 2023 році російські хакерські угруповання продовжують регулярні атаки на український бізнес, що спричиняє колосальні фінансові втрати.

8. Кібервійна: Кібервійна – це серія стратегічних кібератак на національну державу, які завдають їй значної шкоди. Ця шкода може включати виведення з ладу життєво важливих комп’ютерних систем аж до людських жертв. Кібервійна зазвичай визначається як сукупність дій держави або організації, спрямованих на атаку комп’ютерних мережевих систем країн або установ з метою виведення з ладу, пошкодження або знищення інфраструктури за допомогою комп’ютерних вірусів або атак на відмову в обслуговуванні.

Кібервійна може мати різні форми, але всі вони передбачають дестабілізацію або знищення критично важливих систем. Мета – послабити країну-мішень шляхом компрометації її ключових елементів інфраструктури. Прикладами можуть бути атаки на фінансовий сектор, державну інфраструктуру (дамби, енергосистеми), системи безпеки (світлофори, системи раннього попередження), військові ресурси тощо. Кібервійна – це прояв агресії та ворожих дій між державами із застосуванням кіберзброї у новітньому вимірі протистояння – кіберпросторі. Основним фактом відмінності кібервійни від кібертероризму – є скоординовані дії однієї держави, що спрямовані на завдання шкоди комп'ютерним системам і мережам іншої. Кібервійна є частиною військової стратегії держави проти своїх суперників на міжнародній арені, що передбачає використання кіберзброї та проведення спеціальних кібероперацій [49].

Чим більше людство занурюється в кіберпростір та інтегрує його в повсякденне життя, тим більш вразливими стає перед кіберзлочинністю. Цей величезний віртуальний світ не лише пропонує незліченні можливості для зростання та процвітання, але й приховує темні куточки, де можна знайти всі види незаконної діяльності.

2.2. Інформаційна безпека держави: міжнародний досвід

У сучасну епоху стрімкого технологічного розвитку та всеохоплюючої диджиталізації всіх сфер людської діяльності питання захисту прав і свобод на високотехнологічному рівні набуває як ніколи. Інформаційна безпека є пріоритетом для держави з двох ключових причин. По-перше, вона визначає рівень захищеності та стійкості основних сфер життєдіяльності суспільства або країни від шкідливого інформаційного впливу. По-друге, вона впливає на інтенсивність розвитку суспільства в різних галузях завдяки ефективному використанню накопичених людством знань та інформації. Таким чином, належна інформаційна безпека дозволяє країні не тільки захистити себе від

загроз, але й ефективно використовувати інформаційні ресурси для прогресу в різних сферах суспільного життя.

Залежно від конкретного контексту, поняття інформаційної безпеки може розглядатися з різних точок зору. Загалом, інформаційна безпека – це стан захищеності інформаційного середовища суспільства, за якого забезпечується його формування, використання і розвиток в інтересах членів суспільства, установ і організацій та держави [50].

Конфіденційність, цілісність і доступність є фундаментальними принципами інформаційної безпеки. Кожен компонент програми інформаційної безпеки повинен бути створений з урахуванням однієї або декількох з цих концепцій.

Метою застосування заходів конфіденційності є запобігання несанкціонованому розголошенню інформації. Принцип конфіденційності полягає в тому, щоб захистити приватність особистої інформації та гарантувати, що тільки ті особи мають доступ до неї, які потребують її для виконання своїх службових обов'язків.

Захист від небажаних змін даних (додавання, видалення, редагування тощо) є частиною принципу цілісності. Принцип цілісності гарантує, що інформація є правдивою та достовірною і не змінюється – ненавмисно чи навмисно – на помилкову.

Забезпечення здатності системи надавати дані та програмне забезпечення на запит користувача (або в заздалегідь визначений час) називається доступністю. Забезпечення доступності технологічної інфраструктури, додатків і даних, коли це необхідно для внутрішніх бізнес-операцій або для зовнішніх клієнтів, є основною задачею доступності [52].

Інформаційна безпека держави є важливим аспектом національної безпеки, особливо в умовах глобалізації та широкого використання цифрових технологій. Це включає в себе заходи щодо захисту державної інформації, систем та мереж від несанкціонованого доступу, зловживань, витоку інформації та кібератак.

Так, на приклад, політика США у сфері реалізації інформаційної безпеки держави в умовах кіберзлочинності ґрунтується на комплексному підході, який включає законодавчі, технічні та організаційні заходи. За даними офіційного сайту Агентства кібербезпеки та інфраструктурної безпеки (CISA), основними напрямками діяльності це захист федеральних цивільних мереж, кіберпростору та критично важливої фізичної інфраструктури шляхом надання технічної допомоги, оцінки вразливості, управління ризиками та супутніх послуг. Агентство також координує діяльність з кібербезпеки та стійкості через співпрацю та взаємодію з федеральними департаментами, урядами штатів, місцевими, територіальними та племінними урядами, а також приватним сектором. Крім того, CISA відіграє провідну роль у розробці та реалізації національної політики кібербезпеки, здійснює постійний моніторинг кіберзагроз, проводить розслідування інцидентів та виявляє вразливості для захисту від кіберзлочинності на всіх рівнях [71].

З огляду на фундаментальне значення інформаційної безпеки для захисту життєво важливих інтересів громадян, суспільства та держави, забезпечення надійного кіберзахисту є пріоритетом для провідних держав світу.

США. Забезпечення інформаційної безпеки є пріоритетом для Сполучених Штатів Америки з огляду на їхню провідну роль у світовій економіці та геополітиці. Як наддержава з розгалуженою критичною інфраструктурою та потужним високотехнологічним сектором, Сполучені Штати усвідомлюють важливість захисту своїх інформаційних систем від зовнішніх та внутрішніх кіберзагроз.

Так за дослідженнями Центру стратегічних і міжнародних досліджень у червні 2023 року російські хакери здійснили глобальну кібератаку на кілька федеральних агентств США, зокрема на підрозділи Міністерства енергетики. Вони використали вразливість у програмному забезпеченні, яке широко використовується в цих агенціях. У липні цього ж року китайські хакери зламали електронну пошту співробітників Державного департаменту та Міністерства торгівлі США, використовуючи вразливості в системах Microsoft

[72]. Загалом, за 2023 рік кількість кібератак на державні агентства та публічний сектор зросла на 40% у другому кварталі порівняно з першим [73]. Серед найзначніших інцидентів у минулому році була атака на критичну інфраструктуру США, зокрема на об'єкти в Гуамі, яку здійснила група китайських хакерів під назвою Volt Typhoon. Ця кампанія тривала з 2021 року і включала використання законних облікових даних для доступу до систем, що ускладнювало виявлення зловмисників [74]. Атаки програм-вимагачів також завдали значної шкоди державним установам. У період з 2018 по грудень 2023 року понад 423 таких атаки коштували уряду США понад 860 мільйонів доларів США у вигляді простою та витрат на відновлення систем. Наприклад, у травні 2019 року місто Балтимор витратило $18,2 млн на відновлення після атаки з використанням програми-вимагача RobbinHood [75].

Твердження про те, що Сполучені Штати на сьогоднішній день мають найпотужнішу та всеохоплюючу систему управління інформаційною безпекою, не є чимось надзвичайним. Федеральне агентство кібербезпеки та інфраструктури, Рада національної безпеки, Федеральне бюро розслідувань, Агентство національної безпеки, Міністерство оборони та Комісія з цінних паперів і бірж – це ті державні та федеральні органи, які безпосередньо відповідають за інформаційну безпеку та захист державних інформаційних структур та урядових систем у США. Кожна з цих установ і груп має в своїй структурі спеціальний відділ, який займається інформаційною безпекою, запобіганням інформаційним атакам і забезпеченням готовності до кібератак.

США постійно виділяють значні фінансові та матеріальні ресурси на створення та використання передових інформаційних технологій, які дозволяють виявляти та нейтралізувати кіберзагрози. Бізнес та урядові організації тісно співпрацюють з фахівцями з кібербезпеки, щоб знайти та виправити недоліки у своїх системах. Крім того, з метою виявлення, затримання та притягнення до відповідальності осіб, які вчинили кібератаки, уряд Сполучених Штатів постійно налагоджує партнерські відносини з

іноземними державами, правоохоронними органами та комерційним сектором [58].

Франція. З метою переходу до сучасного цифрового суспільства, французький уряд ще у 2015 р. опублікував комплексну національну програму цифрової безпеки, що передбачала реакцію державної системи на зростаючі виклики кіберзлочинності, саботажу, використання даних, шпигунства, поширення пропаганди та неправдивої інформації. Впровадження даної програми здійснювало Французьке Національне агентство з безпеки інформаційних систем (Agence Nationale de la Sécurité des Systèmes d'Information). У співпраці з ANSSI, Міністерством збройних сил Франції, Міністерством внутрішніх справ реалізовувало спільні заходи у сфері міжнародної кіберзлочинності з такими міжнародними організаціями як НАТО, G7 та ОБСЄ [59].

У березні 2023 року сайт нижньої палати французького парламенту - Національних зборів - зазнав потужної DDoS-атаки. Ця кібератака була здійснена хакерською групою з Росії. За даними французьких властей, хакери використовували ботнет, тобто мережу скомпрометованих комп'ютерів та інших пристроїв, для генерації потоку зловмисних запитів, які перевантажили сервери веб-сайту парламенту. Хоча атака тривала всього кілька годин, вона повністю виводила з ладу офіційний сайт Національних зборів протягом цього періоду, роблячи його недоступним для відвідувачів. Французька влада розцінила цю DDoS-атаку як спробу російських хакерів дестабілізувати роботу законодавчого органу Франції. Джерела кібератаки були локалізовані на території РФ. Інциденту передувало загострення дипломатичного конфлікту між Францією та Росією на тлі війни в Україні [96].

У травні 2023 року сталася масштабна кібератака на французьку державну службу зайнятості France Travail (раніше відому як Pôle Emploi). Внаслідок атаки були викрадені персональні дані близько 43 мільйонів осіб, зареєстрованих на сайті служби, включаючи імена, дати народження,

електронні адреси та соціальні номери страхування. Відповідальність за інцидент взяла на себе хакерська група Pandora [97].

У лютому 2024 року дві фірми, що надають послуги медичного страхування – Viamedis та Almerys, стали жертвами кібератак, внаслідок яких персональні дані понад 33 мільйонів осіб були скомпрометовані. Серед викрадених даних були соціальні номери страхування, дати народження та інша особиста інформація, проте банківські реквізити та медичні відомості не постраждали [98].

Франція активно працює над посиленням заходів з кібербезпеки як в межах своїх кордонів, так і по всій Європі. Країна сповнена рішучості реагувати на постійний технічний прогрес в інформаційних системах відповідними заходами безпеки, захищаючи свою критично важливу інфраструктуру та економічні інтереси [59].

Також Україна та Франція підписали угоду 16 лютого 2024 року про співпрацю в галузі кібербезпеки. Відповідно до цієї угоди, сторони працюватимуть над зміцненням спроможності України виявляти, стримувати та запобігати будь-яким кіберзагрозам, кібершпигунству, у тому числі шляхом посилення кіберстійкості та захисту критичної інфраструктури від кібератак. Крім того, Франція надаватиме Україні міжнародну технічну допомогу для модернізації та реформування архітектури безпеки. Сторони також спільно працюватимуть над підвищенням ціни для Російської Федерації та інших ворожих державних і недержавних суб'єктів за безвідповідальне використання кіберможливостей проти України та Франції. Буде посилена операційна співпраця у боротьбі з кіберзлочинністю. Окрім цього, угода передбачає поглиблення співробітництва України зі структурами ЄС та НАТО у сфері кібербезпеки [76].

Німеччина. У Федеративній Республіці Німеччина не існує єдиного законодавчого документу, який би регулював питання кібербезпеки та захисту даних. Натомість це питання регулюється поєднанням федерального та європейського законодавства. Як і в інших країнах-членах ЄС, захист

персональних даних у Німеччині забезпечується виконанням суворих вимог Загального регламенту ЄС про захист даних. Спробою Німеччини модернізувати законодавчу базу у сфері кібербезпеки стало прийняття закону 18 травня 2021 року про IT-безпеку 2.0. Цей нормативний акт покликаний посилити безпеку інформаційних систем і гармонізувати інші закони про кібербезпеку, щоб протистояти постійно мінливому ландшафту цифрових загроз і проблем кібербезпеки, таких як збільшення кількості атак з вимогами викупу. Порушення законодавства у сфері кібербезпеки загрожує організаціям, підприємствам штрафами до 20 мільйонів євро або 4% від їхнього річного глобального обороту. На сьогоднішній день найбільший штраф у сфері кібербезпеки був накладений у Німеччині й склав 35 мільйонів євро, які заплатила шведська компанія H&M за незаконну обробку конфіденційних даних співробітників [60].

У лютому 2023 року російська хакерська група Killnet здійснила масовану DDoS-атаку на ряд німецьких сайтів, включаючи аеропорти, поліційні мережі та фінансові установи. Ця атака була відповіддю на рішення Німеччини постачати Україні танки Leopard 2. Попри значні перебої в роботі вебсайтів, суттєвих наслідків для роботи цих установ не було зафіксовано [100].

Також у березні 2023 року хакери здійснили кібератаку на сайти німецького парламенту, що спричинило тимчасове вимкнення вебсайтів. Хакерська група, пов’язана з російськими інтересами, знову ж таки була відповідальною за ці дії, що вважається частиною ширшої кампанії з дестабілізації європейських країн, які підтримують Україну[101].

Забезпечення інформаційної безпеки є актуальним питанням для впливових міжнародних організацій та альянсів. Зростаюча взаємозалежність і взаємопов’язаність світу в епоху глобалізації вимагає координації зусиль на наднаціональному рівні для протидії транскордонним кіберзагрозам.

НАТО. Після повномасштабного вторгнення Росії в Україну у 2022 році НАТО посилила свої зусилля з протидії російським кібератакам. Організація запровадила нову програму швидкого реагування на кібератаки, яка передбачає

посилення координації та обміну розвідданими між членами НАТО. У червні 2022 року НАТО оголосило про створення «віртуального швидкого кібернетичного реагування» для протидії російським кіберзагрозам, зокрема у відповідь на численні атаки на Україну.

Крім того, НАТО надала Україні окремий пакет допомоги у сфері кібербезпеки, щоб підтримати її у захисті від кіберінцидентів. Також були зроблені кроки для посилення кіберзахисту критично важливої інфраструктури та підвищення спільної обізнаності про кіберзагрози серед членів Альянсу [77].

У НАТО наголосили, що кібератака потенційно може спричинити застосування статті 5 Північноатлантичного договору, яка передбачає колективну оборону в разі нападу на члена Альянсу. Це демонструє серйозність, з якою НАТО сприймає кіберзагрози, особливо з боку Росії [78]. Першочерговим завданням НАТО є запобігання і захист шляхом посилення власних оборонних сил і засобів, тому Альянс постійно працює над розбудовою стійкості до загроз безпеці в різних сферах. У 2017 р., міністри оборони країн-членів організації схвалили оновлену версію Плану дій з кіберзахисту і «дорожню карту» для кіберпростору. Ця дорожня карта мала на меті розробити і забезпечити оперативний потенціал для протидії кіберзагрозам або кібератакам, таким чином задовольняючи потреби в обороні і стійкості альянсу. Зрештою, ця дорожня карта призвела до створення Верховного головнокомандування Об'єднаних збройних сил НАТО в Європі (SHAPE) в Монсі, Бельгія, яке прагнуло надавати підтримку членам Альянсу в галузі кіберзахисту. Зокрема, до складу SHAPE увійшов Центр операцій в кіберпросторі, діяльність якого спрямована на моніторинг міжнародного інформаційного простору, а також підготовку військових та цивільних ресурси до можливих потенційних військових сценаріїв.

На саміті НАТО в Брюсселі в 2018 р. Альянс створив новий Центр кібернетичних операцій з метою підвищення рівня кібербезпеки як центрального елемента командної структури НАТО. У 2021 р. НАТО призначила свого першого Головного офіцера з питань інформації для

сприяння інтеграції, узгодженню і згуртованості систем інформаційно-комунікаційних технологій в усій організації. Таким чином, кібербезпека стала пріоритетом для НАТО, в тому числі захист критично важливої інфраструктури від шкідливого програмного забезпечення і методів вторгнення [53]. У рамках цих ініціатив НАТО забезпечує стійкість кібермереж за допомогою військової освіти, навчань та інших засобів оперативної координації і синхронізації.

Так, на саміті НАТО в Брюсселі в 2021 р. була створена Комплексна політика кіберзахисту, що враховує головну місію Альянсу: загальна політика стримування і оборони. Вкотре було підкреслено рішучість союзників ефективно протидіяти кіберзагрозам військовими, політичними і дипломатичними засобами. Визнано, що суттєві кібернетичні дії можуть розглядатися як акт війни. Було наголошено на необхідності співпраці на політичному, військовому і технологічному рівнях щодо дотримання міжнародного права та просування глобальної стабільності в кіберпросторі. Після початку повномасштабного вторгнення Росії в Україну у 2022 році, НАТО значно посилило свою реакцію на російські кібератаки. Альянс зосередився на підвищенні стійкості своїх кіберзахисних систем та поліпшенні координації між країнами-членами для швидшого обміну розвідданими та спільного реагування на загрози. Було збільшено кількість кібернавчань та розширено співпрацю з приватним сектором для обміну інформацією про кіберзагрози. НАТО також підтримує Україну в її зусиллях із захисту від кібератак, надаючи технічну допомогу та експертні консультації [77].

Під час Вільнюського саміту НАТО 2023 р. Альянс схвалив нову концепцію кіберзахисту, що передбачає з метою посилення міжнародної стабільності в кіберпросторі посилення національних системн кіберзахисту, особливо критично важливої інфраструктури. Також було започатковано нові ініціативи щодо співпраці у виявленні та протистоянні кіберінцидентам на міжнародній арені [54].

ОБСЄ. Організація з безпеки та співробітництва в Європі також відіграє свою роль у зміцненні кібербезпеки та безпеки інформаційно-комунікаційних

технологій, зокрема шляхом мінімізації ризиків виникнення конфліктів між державами внаслідок використання ІКТ. Ключовим завданням у цій сфері є імплементація на регіональному рівні відповідних керівних принципів, розроблених групами урядових експертів під егідою Організації Об'єднаних Націй. Для подолання викликів держави-учасниці ОБСЄ працюють над розробкою заходів зі зміцнення довіри, покликаних зменшити ризики конфліктів, пов'язаних з ІКТ. Ці заходи спрямовані на підвищення передбачуваності кіберсередовища і пропонують конкретні інструменти та механізми для уникнення непорозумінь:

– механізм залучення держав до консультацій щодо потенційних інцидентів у сфері кібербезпеки/ІКТ з метою деескалації зростаючої напруженості;

– платформа для обміну думками, національними підходами до кібербезпеки/безпеки ІКТ, що сприятиме кращому розумінню намірів держав у кіберсередовищі;

– конкретні завдання, такі як захист критичної інфраструктури на основі ІКТ, що дозволить державам-учасницям спільно підвищувати кіберстійкість в регіоні ОБСЄ на загальну користь.

Окрім заходів зі зміцнення довіри у сфері кібер/ІКТ-безпеки, ОБСЄ та її інститути також зосереджені на протидії загрозам у цій сфері з боку недержавних суб'єктів, таких як організована злочинність і терористичні угруповання. Ключовим напрямком роботи є сприяння адекватному і своєчасному реагуванню національних органів влади на ці загрози, шляхом вдосконалення криміналістики та впровадження інноваційних підходів для запобігання використанню терористами ІКТ в якості тактичного інструменту [55].

Європейський Союз. ЄС також створив спеціалізовану агенцію, яка стала провідним експертним центром з кібербезпеки на континенті. Офіційна назва цієї установи – Агентство Європейського Союзу з мережевої та інформаційної

безпеки або ж ENISA. Штаб-квартира Агентства знаходиться в грецькому місті Іракліон на острові Крит, а операційний офіс – в Афінах.

З моменту свого заснування у 2004 році ця організація активно працює над забезпеченням високого рівня безпеки мереж та інформаційних систем в межах Європейського Союзу. Її діяльність спрямована на формування культури інформаційної безпеки в суспільстві та підвищення обізнаності громадськості з цього питання, що сприяє належному функціонуванню спільного ринку ЄС [56].

Основними обов’язками ENISA є надання консультацій та допомоги Європейській Комісії та державам-членам ЄС з питань інформаційної безпеки, включаючи діалог з промисловістю для вирішення проблем безпеки в апаратному та програмному забезпеченні. Агентство збирає та аналізує дані про інциденти кібербезпеки в Європі та ризики, що виникають, сприяє оцінці ризиків та розробляє методи управління ризиками для підвищення стійкості до кіберзагроз. Крім того, ENISA працює над підвищенням обізнаності та співпраці між різними суб'єктами у сфері інформаційної безпеки, зокрема шляхом розвитку державно-приватного партнерства з промисловістю.

Діяльність агентства зосереджена на чотирьох ключових напрямках: команди реагування на комп’ютерні інциденти, захист та стійкість критичної інформаційної інфраструктури, ідентичність та довіра, а також управління ризиками. ENISA допомагає державам-членам у створенні та управлінні CERT, надає рекомендації та розробляє найкращі практики для інституцій ЄС, Європейської комісії, національних регуляторів та приватного сектору у сферах планування на випадок надзвичайних ситуацій, стратегій кібербезпеки, мінімальних заходів безпеки для інтернет-провайдерів, національних кібервиборів, взаємопов’язаних мереж, хмарних обчислень тощо. Агентство також працює над підвищенням довіри користувачів до онлайн-сервісів і сприяє взаємному визнанню механізмів електронної ідентифікації та автентифікації електронного підпису між країнами-членами ЄС [57].

У рамках спільних зусиль з посилення кібербезпеки Європи Європейський союз у травні 2022 р. виступив з ініціативою, яка об’єднала три найважливіші спільноти з кібербезпеки: Мережу організацій зв’язку з кіберкриз, Мережу команд реагування на інциденти комп'ютерної безпеки і Групу співробітництва з мережевих та інформаційних систем. Ці групи, а також Європейська комісія і ENISA об’єдналися заради спільної мети – зміцнення кібербезпеки на європейському континенті.

РОЗДІЛ ІІІ.
КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

3.1 Кіберфронт: кіберзлочинність в Україні під час повномасштабної війни

Одним із найпотужніших інструментів сучасної війни та конфлікту є інформаційна війна. Росія активно використовує весь спектр інформаційних стратегій і тактик, щоб досягти своїх цілей, одночасно знищуючи єдність і стабільність України. Хоча інформаційна агресія почалася задовго до відкритого військового вторгнення, вона набула безпрецедентних масштабів і інтенсивності саме після 24 лютого 2022 року.

Росія використовує різноманітні деструктивні інформаційні кампанії, включаючи традиційну пропаганду та дезінформацію, а також складні кібератаки та підривну діяльність. Зусилля мають на меті послабити українську державу зсередини, підірвати довіру громадян до влади, посіяти сумніви та розбрат у суспільстві та погіршити імідж України на міжнародній арені. Росія веде гібридну війну проти нашої країни через інформаційний фронт.

Ще до початку повномаштобного вторгнення, 14 січня 2022 року відбулася масштабна кібератака на державні веб-ресурси України. Зловмисники здійснили дефейс (тип хакерської атаки, при якій сторінка вебсайту замінюється на іншу [79]) близько 70 вебсайтів державних установ, які використовували систему керування контентом October CMS, розроблену компанією Kitsoft. На цих сайтах було розміщене провокаційне повідомлення трьома мовами про помсту українцям за історичні події, що вказувало на можливий російський слід атаки.

Успішно реалізувати кібератаку вдалося через відому вразливість October CMS, виявлену ще у 2021 році. У результаті хакерського нападу не працювали офіційні сайти міністерств, відомств, Міноборони, МЗС, ДСНС, та сервіс

державних послуг «Дія». Речник міністра, відповідального за польську розвідку, Станіслав Жарин заявив, що кібератаки, про які повідомляє українська сторона, є характерними для діяльності спецслужб Російської Федерації. Лише 16 січня вдалося відновити роботу більшості уражених ресурсів, окрім деяких критично важливих, зокрема порталу «Дія» [80].

15 лютого розпочалась нова масштабна DDoS-атака на українські державні та банківські інтернет-ресурси.

Протягом понад 5 годин хакери обстрілювали потужним мережевим трафіком сайти близько 15 провідних банків, зокрема «ПриватБанк» та «Ощадбанк», а також урядові онлайн-ресурси у домені gov.ua.

У результаті атаки тимчасово припинили роботу вебсайти «ПриватБанку», «Ощадбанку», Міноборони, Збройних Сил та Мінреінтеграції. Проте, завдяки оперативній допомозі США вдалося швидко відбити напад. Згодом, 16 лютого, основні банківські сайти вже відновили роботу [81].

За словами міністра цифрової трансформації Михайла Федорова, ця DDoS-атака стала наймасштабнішою в історії України та коштувала мільйони доларів.

Водночас, низка технічних фахівців зазначили, що потужність нападу була не такою високою, а його вартість оцінювалась у декілька тисяч доларів, оскільки така атака не завдасть суттєвої шкоди сучасному серверному обладнанню середнього рівня [82].

За день до повномасштабного вторгнення Росії в Україну 24 лютого 2022 року розпочалася нова хвиля кібератак на державні установи та банківський сектор. Хакери завдали удару по вебресурсам Верховної Ради, Кабінету Міністрів, МЗС та інших відомств. Міносвіти попереджувально відключило свій сайт.

Згідно з повідомленнями міністра цифрової трансформації Михайла Федорова, портал «Дія» успішно протистояв атаці.

Пізніше з’ясувалося, що постраждали також сайти СБУ, міністерств інфраструктури й аграрної політики. На ресурсі останнього з’явився той самий дефейс, що й під час нападу 14 січня [83].

Компанія ESET виявила, що після DDoS-атаки на зламані сайти було впроваджено шкідливе ПЗ HermeticWiper для знищення баз даних. Воно було скомпільоване ще 28.12.2021, хоча атака сталася 23.02.2022 [84].

Вночі 24.02.2022, коли розпочалося вторгнення, сайт Київської ОДА зазнав хакерського нападу [85].

На ресурсах i.ua та meta.ua були виявлені масові фішингові розсилки на приватні адреси українських військових від білоруської хакерської групи UNC1151, пов’язаної з міноборони Білорусі [86].

За даними Державної служби спеціального зв’язку та захисту інформації України, в 2022 році кількість кібератак на інформаційну інфраструктуру нашої держави зросла майже втричі порівняно з 2021 роком. Водночас на 26% збільшилась кількість інцидентів, джерело яких пов’язують з Росією.

У другому кварталі 2022 року основними цілями російських хакерських угруповань стали українські ЗМІ, уряд та місцеві органи влади.

Порівняно з першим кварталом, протягом другого кварталу 2022 року на 38% зросла кількість подій, пов’язаних з розповсюдженням шкідливого програмного забезпечення.

Це свідчить про значне підвищення рівня шкідливої активності в мережі, спрямованої на поширення вірусів та спроби використати вже заражені пристрої для формування ботнетів [87].

Розподіл кіберзлочинності в Україні за типами впродовж другого кварталу 2022 року можна побачити на Рисунку 3.1.

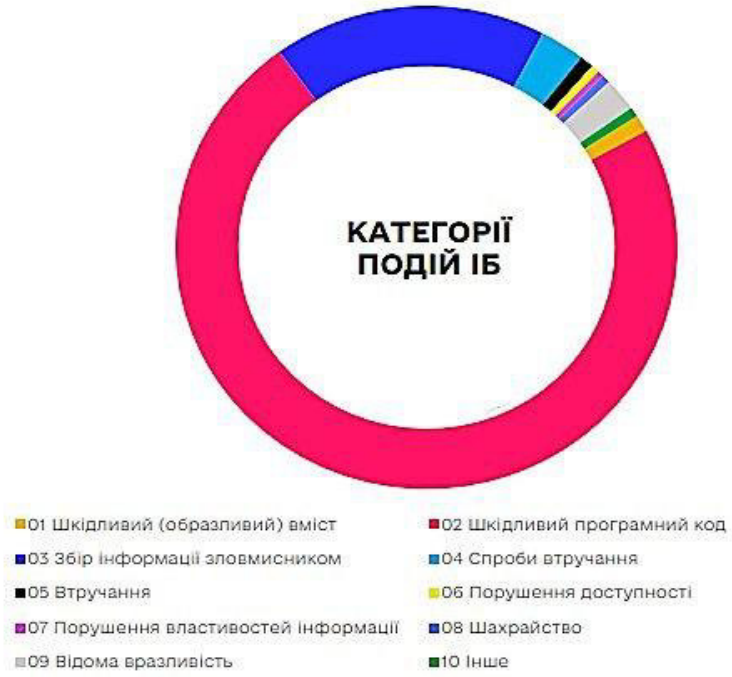

Рис.3.1.Розподіл кіберзлочинності в Україні за типами

У третьому кварталі 2022 року кількість критичних кіберінцидентів, пов'язаних з російськими IP-адресами, зросла у 35 разів порівняно з попередніми кварталами. Також майже вдвічі збільшилась кількість виявлених атак з активним скануванням з російських IP. Саме з цих адрес здійснювались напади на українські ресурси, поширювалась дезінформація проти державних органів.

Найбільше інцидентів пов'язано з IP з США, проте геолокація не завжди вказує на реальне джерело. За атрибуцією, більшість кіберінцидентів організовані хакерськими угрупованнями на кшталт Gamaredon, які фінансуються російським урядом [88].

Розподіл кіберзлочинності в Україні за типами впродовж третього кварталу 2022 року можна побачити на Рисунку. 3.2.

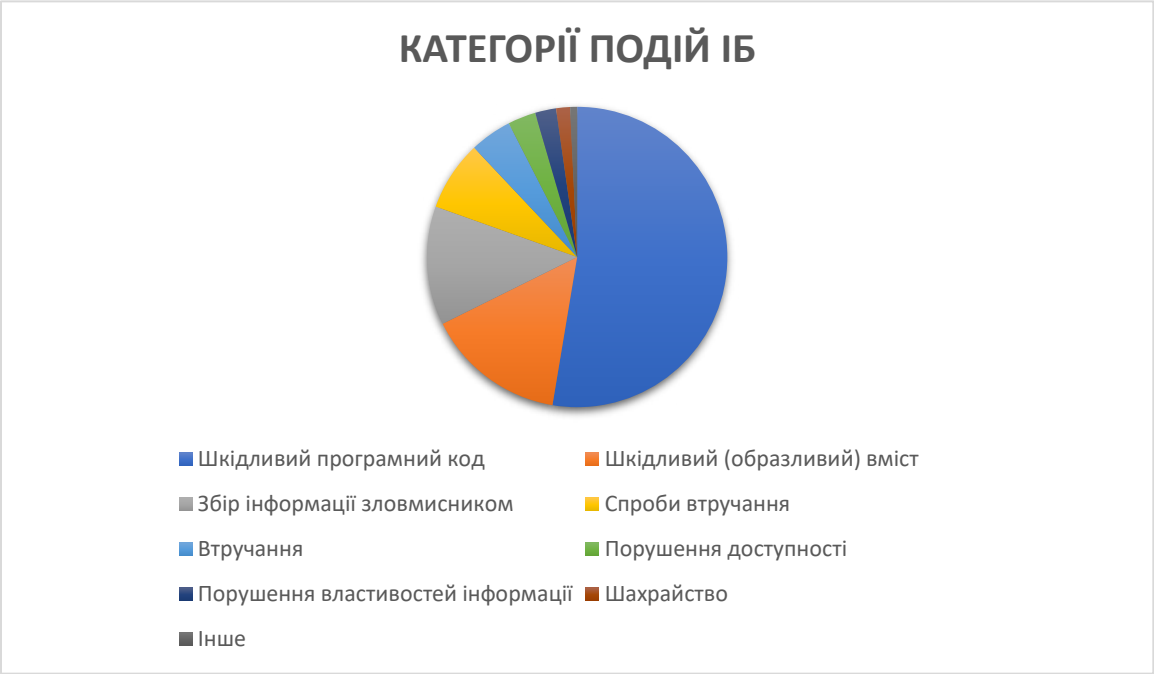

Рис.3.2.Розподіл кіберзлочинності в Україні за типами

У третьому секторі 2022 року російські хакери були активні в широкому спектрі секторів. Найбільш активними вони є в фінансовому, комерційному секторі безпеки, ЗМІ, урядових та місцевих органах влади. (Див. рис.3.3)

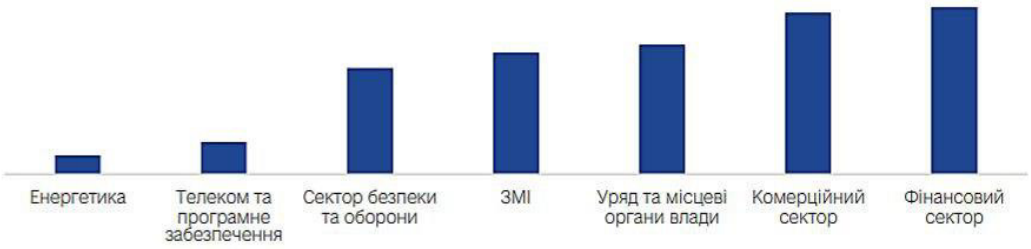

Рис.3.3.Активність російських хакерських угрупувань за секторами

Хакерські атаки на фінансовий та комерційний сектори безпеки, засоби масової інформації, органи державної влади та місцевого самоврядування є надзвичайно небезпечними, оскільки можуть призвести до розкрадання коштів, порушення роботи банків та платіжних систем, спричинити економічну нестабільність та витік конфіденційних даних клієнтів.

У комерційній сфері злом корпоративних мереж може призвести до крадіжки комерційної таємниці, інтелектуальної власності, порушення

виробничих ланцюжків, що може спричинити значні фінансові збитки та втрату конкурентоспроможності.

Атаки на ЗМІ можуть бути використані для поширення дезінформації, пропаганди та маніпулювання громадською думкою, підриву довіри до ЗМІ та дестабілізації ситуації. А успішні кібератаки на органи державної влади та місцевого самоврядування можуть паралізувати роботу державних установ та систем надання послуг, спричинити витік конфіденційних даних державного значення, що загрожує національній безпеці та суверенітету країни в цілому.

Протягом 2022 року після 24 лютого урядовий підрозділ кіберінцидентів CERT-UA зареєстрував та опрацював понад 2100 з 7000 атак З них 120 були спрямовані на фінансовий сектор, 156 – на комерційні організації, а 92 – на телекомунікаційні компанії та IT-розробників [89] (Див.рис.3.4)

Рис.3.4.Сектори кібератак протягом 2022 року

За словами технічного директора IT-компанії UNITY-BARS Олега Музики, після США Україна стала другою найбільш атакованою країною світу у 2022 році. У порівнянні з 2021 роком кількість кібернападів на фінансові установки зросла в 3,5 рази і становить близько 5% від їхньої загальної кількості. На IT-галузь припадає близько 10% всіх хакерських атак минулоріч [89].

Експерти UNITY-BARS констатують великий сплеск кібератак в Україні протягом 2022 року на тлі повномасштабної війни з Росією. Упродовж 2023 року система кібербезпеки України опрацювала величезний масив даних – близько 18 мільярдів подій, отриманих шляхом моніторингу та аналізу телеметричної інформації про кіберінциденти та атаки. З цього величезного обсягу первинний аналіз виявив 133 мільйони підозрілих подій у сфері інформаційної безпеки.

Після ретельної обробки та повторного аналізу цих підозрілих подій було зафіксовано 148 тисяч критичних інцидентів інформаційної безпеки, які були розцінені як потенційні кіберінциденти. Окрім автоматизованого виявлення, аналітики безпеки особисто зареєстрували та опрацювали 1105 кіберінцидентів.

Цей показник на 62,5% вищий, ніж у 2022 році, що свідчить про значне зростання кіберзагроз для українських інформаційних систем у 2023 році.

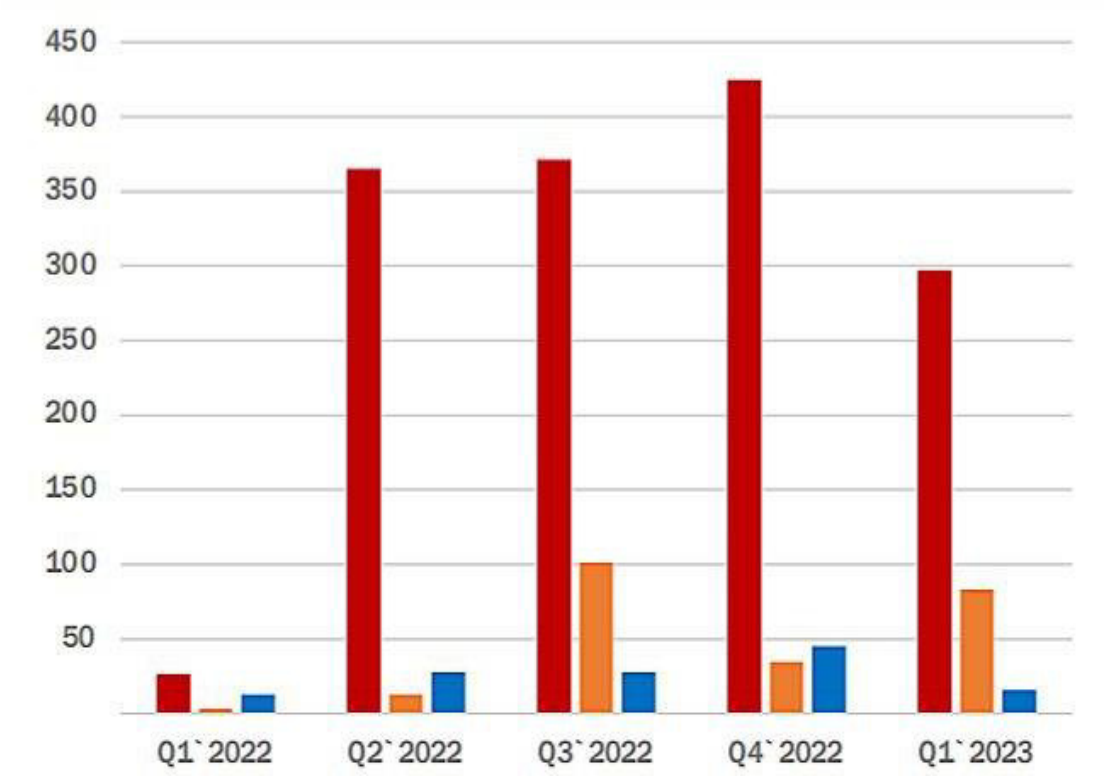

Рис.3.5.Динаміка активності проросійських хакерських угрупувань за типами атак у кварталах 2022 року

Аналізуючи діаграму на рисунку 3.5 з даними про динаміку активності проросійських хакерських груп за різними типами атак від Державного центру

кібербезпеки, одразу кидається у вічі певна тенденція. Порівняно з четвертим кварталом минулого року, на початку 2023-го загальна кількість кібернападів, які організовують проросійські хактивісти, дещо зменшилася.

Проте не варто применшувати цю загрозу, адже незважаючи на деяке скорочення масштабів, систематичність та інтенсивність таких атак залишились на вкрай високому рівні небезпеки. Хакерські угруповання, підконтрольні Російській Федерації, ні на мить не припинили спроб завдати удару по українських інформаційних системах та онлайн-ресурсах.

У першій чверті 2023 року система моніторингу та аналізу кіберзагроз в Україні виявила величезну кількість потенційно небезпечних випадків. На етапі первинного аналітичного скринінгу було відфільтровано 7 мільйонів підозрілих подій, пов’язаних з інформаційною безпекою. Після ретельного вторинного аналізу та верифікації цих тривожних сигналів, експерти кібербезпеки класифікували 34 тисячі з них як критичні інциденти, що становили реальну загрозу і потребували невідкладного реагування.

Окрім автоматизованого виявлення, безпосередньо аналітиками було ідентифіковано, задокументовано та опрацьовано 202 випадки успішних кібератак та порушень інформаційної безпеки протягом першого кварталу поточного року.

Ці числа демонструють масштаби кіберзагроз, з якими продовжувала стикатися Україна на тлі тривалого збройного конфлікту та гібридної війни з Росією в кіберпросторі.

У першому кварталі 2023 року основну частку хакерської активності проросійських хактивістських угруповань забезпечили кілька найбільш організованих і вмотивованих груп. Згідно зі статистикою, близько 90% усіх атак такого типу, зафіксованих за звітний період, здійснили XakNet, NoName057(16), RussianHackersTeam, RaHDit та Free Civillian[90] (Рис.3.6.)

Аналізуючи діаграму активності хакерських угруповань у різні періоди першого кварталу 2023 року, можна виділити декілька піків. Найінтенсивніша діяльність групи Free Civillian спостерігалася з 19 по 26 лютого. Угруповання

XakNet було найбільш активним з 15 по 22 січня. Щодо RaHDit, то його пік припадав на період з 22 по 29 січня. А команда RussianHackersTeam досягла максимальної активності наприкінці першої чверті року.

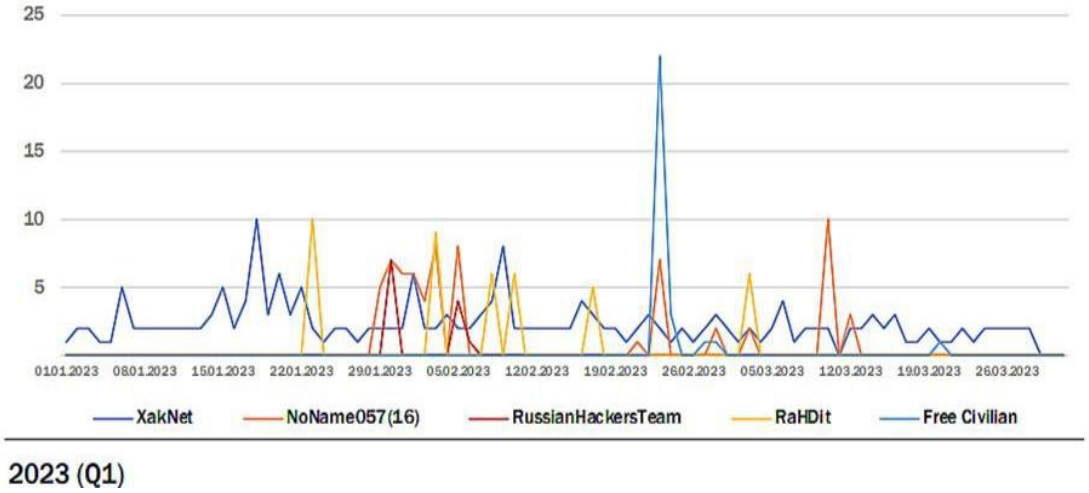

Рис.3.6. Динаміка активності проросійських хакерських угрупувань

Ці найпотужніші проросійські хакерські угруповання, вочевидь, розглядають Україну як пріоритетну ціль для ворожих кібероперацій і не полишають спроб завдати максимальної шкоди інформаційним системам та ресурсам країни. Їх деструктивна діяльність вимагає підвищеної пильності та жорсткої протидії з боку українських фахівців з кібербезпеки.

Масштаби та інтенсивність атак основних гравців кібервійни на боці Росії вкотре демонструють серйозність загроз, з якими Україна продовжує стикатися у віртуальному просторі на тлі повномасштабного збройного протистояння.

У другому кварталі 2023 року система виявлення та реагування на кіберзагрози в Україні опрацювала величезний масив даних – 3 мільярди подій, отриманих шляхом моніторингу та аналізу телеметричної інформації про можливі інциденти та атаки.

На етапі первинного аналізу було виявлено 122 мільйони підозрілих випадків, пов’язаних з порушенням інформаційної безпеки. Після ретельної фільтрації та повторної експертної оцінки статус критичних інцидентів, які вимагали негайного реагування, отримали 55 тисяч таких подій.

Окрім автоматизованого виявлення, безпосередньо фахівцями-аналітиками було задокументовано та опрацьовано 191 випадок успішних кібератак.

Порівняно з першим кварталом, у другій чверті спостерігалося значне зростання кількості інцидентів інфобезпеки за категоріями «шкідливе ПЗ» (на 95,8%) та «збір інформації зловмисниками» (на 35,8%). Загалом число критичних подій зросло на 38,1% [91]. Ці числа демонструють, що весняний період 2023 року був позначений серйозною активізацією кіберзагроз для України в контексті тривалого збройного конфлікту.

У другому кварталі 2023 року основний удар проросійських хакерських угруповань хактивістів взяли на себе кілька найбільш потужних команд. За даними статистики, приблизно 89% усіх виявлених протягом звітного періоду атак цього типу були організовані колективами "Народная CyberАрмия", "WE ARE BlOODNET", "Солнцепек", "Xaknet" та "NoName057(16)". Див.рис.3.7.

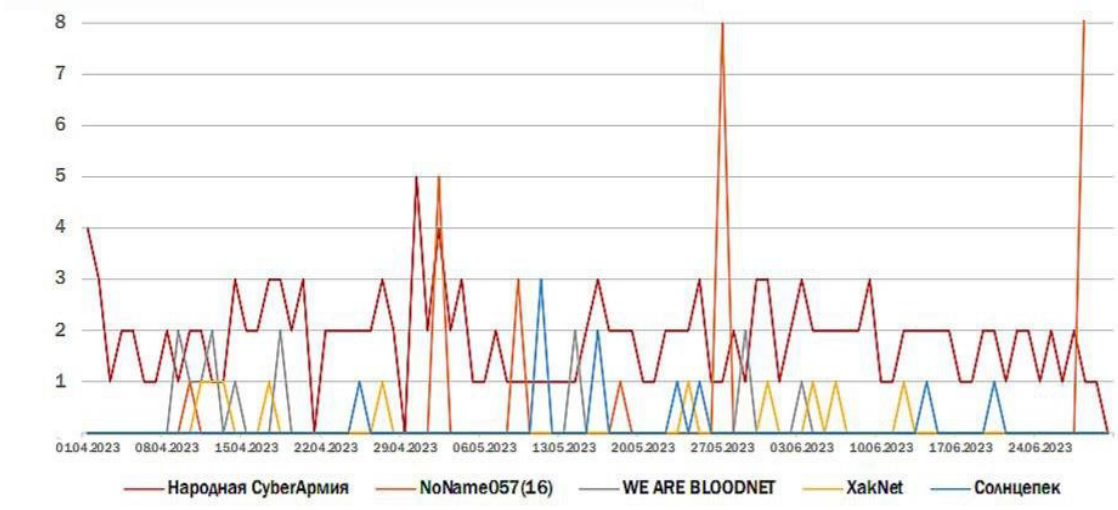

Рис.3.7. Динаміка активності проросійських хакерських угрупувань

У період з 29 квітня по 3 червня 2023 року найактивнішим кіберугрупованням, згідно з даними діаграми, виявилася «Народная CyberАрмия», яка демонструвала найвищу активність. Також помітну активність проявили угруповання «WE ARE BLOODNET» та XakNet, чиї показники на діаграмі були трохи меншими, але все одно значимими. В той час як угруповання «Солнцепек» було особливо активним у кібератаці з 10 по 29 квітня 2023 року, після цього періоду їхня активність відчутно зменшилася.

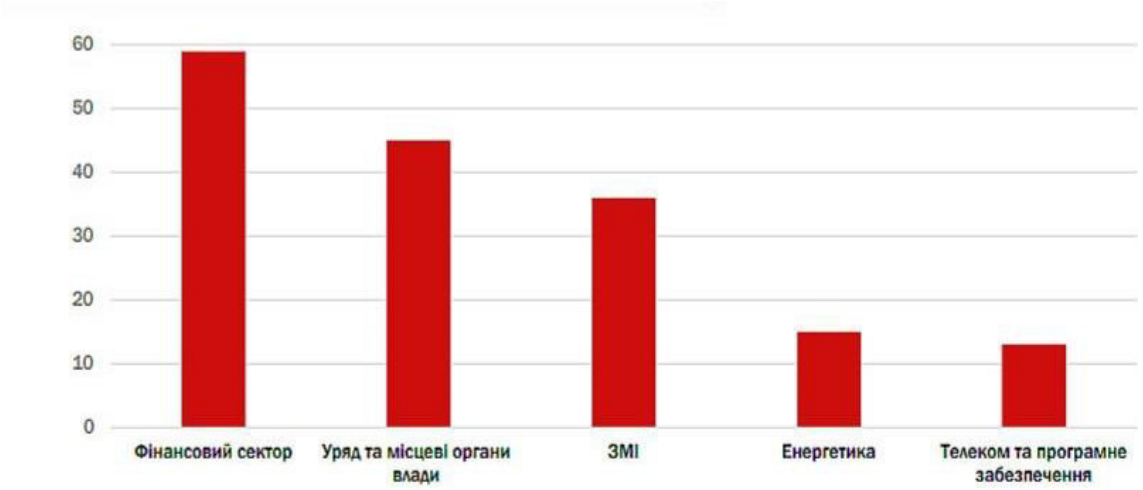

Рис.3.8. Розподіл активності проросійських хакерських угрупувань за секторами

Згідно з аналітичними матеріалами, підготовленими фахівцями Національного координаційного центру кібербезпеки, протягом звітного періоду найбільше кібератак зосереджувалося на низці критично важливих галузей національної інфраструктури.(Рис.3.8.)

Основний удар проросійських хакерів прийшовся на фінансову систему держави, урядові інформаційні ресурси, медійний сектор, а також підприємства енергетичної та телекомунікаційної сфер. Очевидно, ворожа сторона прагнула максимально паралізувати функціонування ключових секторів, завдавши руйнівного удару по їхніх цифрових системах і мережах.

Така концентрація атак на стратегічно важливих напрямках є невипадковою та засвідчує, що кібернетичні операції розглядаються агресором як один із пріоритетних інструментів для досягнення воєнно-політичних цілей шляхом дестабілізації ситуації всередині України.

У третьому кварталі 2023 року система виявлення кіберзагроз в Україні зафіксувала 1,5 мільйона підозрілих випадків на етапі первинного аналізу. Після ретельної фільтрації та верифікації даних статус критичних інцидентів із потенційною загрозою для інфобезпеки отримали 12 тисяч таких подій. Крім автоматизованих систем, безпосередньо аналітиками було задокументовано 355 успішних кібератак. Порівняно з другим кварталом, у третій чверті спостерігалося зростання зареєстрованих кіберінцидентів на 46%. Протягом

звітного періоду система реагування розширила моніторинг, додавши 14 нових об’єктів з урядового, енергетичного та військового секторів.

За цей час фахівці оперцентру проаналізували 957 фішингових атак різного типу: викрадення автентифікаційних даних (507 випадків), розсилка шкідливих вкладень (340), кіберздирництво (108) та експлуатація вразливостей (2). При цьому 80% атак на крадіжку акаунтів використовували легітимні сервіси та технології.

Найактивнішими організаторами кібернападів виступали проросійські угрупування «Народная CyberАрмия», «BLUENET», «NoName057(16)», «PHOENIX» та «Lira», на частку яких припадало близько 90% усіх зафіксованих атак. Їхні зусилля були зосереджені переважно на фінансовому, урядовому, телекомунікаційному, освітньому секторах та громадянському суспільстві.[92] (Див.рис.3.9.)

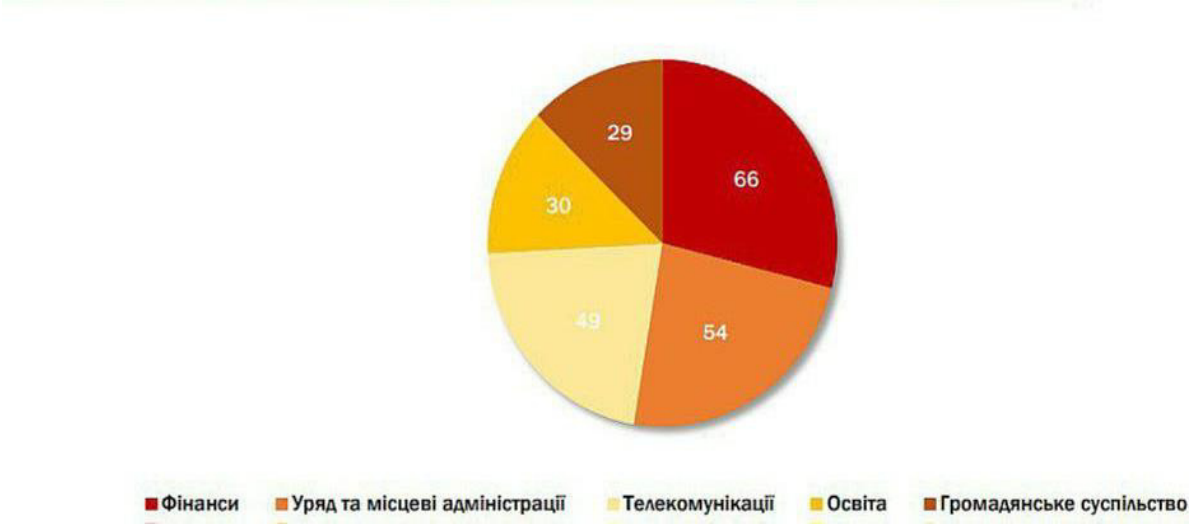

Рис.3.9.Динаміка активності проросійських хакерських угрупувань за тарнетованими секторами

Фінансовий сектор зазнав найбільшої шкоди внаслідок кібератак проросійських хакерських угруповань. Цей сектор є пріоритетною ціллю для кіберзлочинців через можливість викрадення коштів, дестабілізації платіжних систем та підриву репутації фінансових установ.

Системи кібербезпеки України опрацювали 1,4 мільярда подій у четвертому кварталі 2023 року за допомогою моніторингу та аналізу телеметрії

про потенційні інциденти та атаки. На першому етапі аналізу було виявлено 2 мільйони підозрілих випадків інформаційної безпеки. Після ретельного фільтрування було визначено 46 тисяч подій, які експерти вважали потенційними кіберзагрозами.

Аналітики задокументували 357 успішних кібератак, окрім автоматизованих систем. Протягом звітного періоду моніторинг розширився, і ще один об’єкт з урядового сектору був підключений до системи реагування. Загальна кількість об’єктів кіберзахисту зросла порівняно з третім кварталом: збір мережевої телеметрії зріс на 7, захист кінцевих точок зріс на 6, сканування вразливостей зросла на 5.

Фахівці оперативного центру виявили 1731 фішингову атаку протягом четвертої чверті. Ці атаки включали викрадення автентифікаційних даних (672 випадки), розсилку шкідливих вкладень (472), а також кіберздирництво (587).

Загалом у четвертому кварталі було зафіксовано на 26% менше кібератак, організованих проросійськими угрупованнями. Це продовжило тенденцію загального зниження кількості нападів на українські організації з початку 2023 року. Тим часом атаки були розподілені рівномірно протягом кварталу, не спостерігаючи значних змін у частоті та інтенсивності атак [93].

Близько 91% усіх задокументованих кібернападів були організовані групами «Народна CyberАрмія», «RU_DDOS C2», «Layer Legion (DDoS Legion), «NoName057(16)» та «Vосход». Рис.3.10.

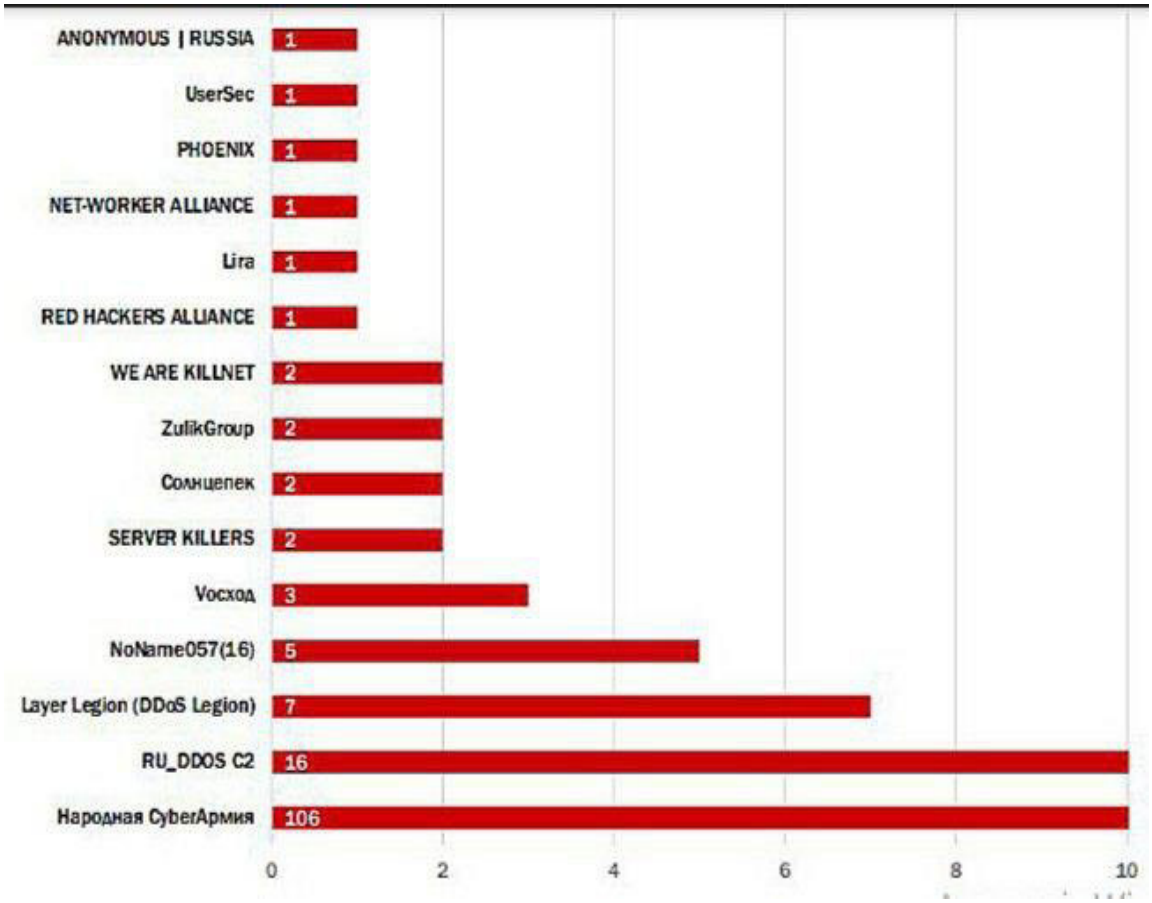

Рис.3.10. Найактивніші проросійські угруповання хактивістів

Телекомунікації, уряд, фінанси, оборона та енергетика були головними сферами уваги хактивістів. (Див.Рис.3.11)

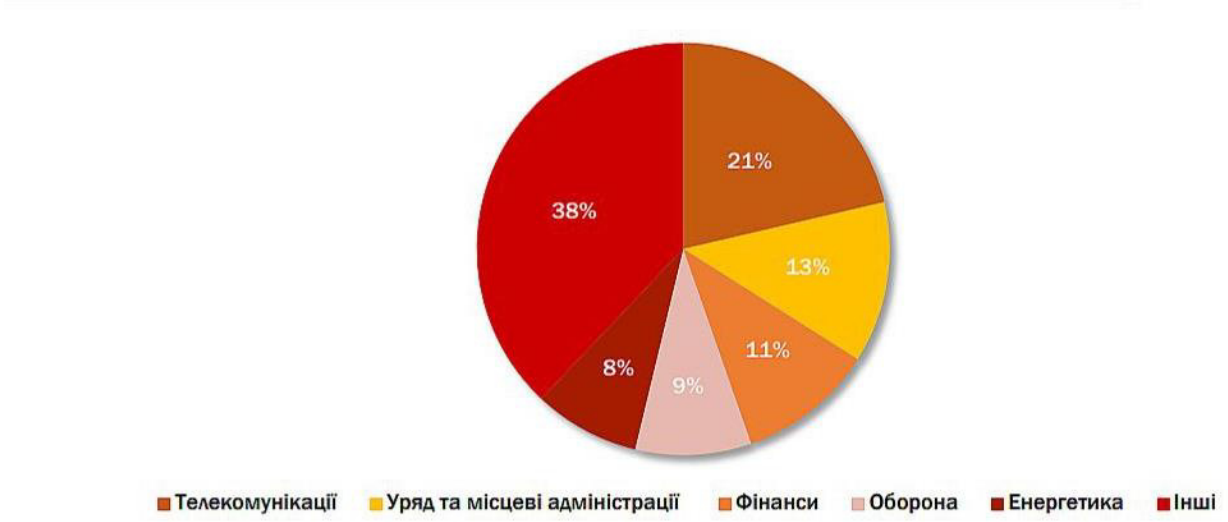

Рис..3.11. Динаміка активності проросійських хакерських угрупувань за таргетованими секторами

Атаки на телекомунікаційний сектор можуть спричинити значні перебої в комунікаціях, що матиме суттєвий вплив на всі аспекти життя суспільства та бізнесу, включно з екстреними службами та фінансовими операціями. Такі ж атаки, якщо вони вразять урядові та оборонні системи, можуть призвести до витоку конфіденційної інформації, перешкодити військовим і стратегічним операціям та підірвати довіру до урядових інституцій. Крім того, систематичні кібератаки на фінансовий сектор створюють ризик значних фінансових втрат, порушення роботи банківських систем і втрати клієнтських даних, що знижує довіру до фінансових установ. Атаки на енергетичний сектор можуть призвести до масштабних відключень електроенергії та пошкодження інфраструктури, що спричинить значні економічні збитки та вплине на критичні аспекти життя.

Назар Тимошик, фахівець Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, розповів про свої думки щодо майбутніх викликів на конференції SANS CyberThreat 2023 у Лондоні. Він заявив, що Україна повинна очікувати більш складних кібератак з боку російського агресора, зокрема тих, що включають штучний інтелект. Він підкреслив, що російська сторона активно готує нове покоління хакерів, що може призвести до зростання і складності кіберзлочинів проти України у 2024 році. Однак з 2022 року Україна підвищила свою кіберзахищеність, зокрема завдяки обміну інформацією та технічній підтримці. Це призвело до того, що українські компанії стали більш професійно реагувати на кіберризики [94].

Повномасштабна агресія Росії проти України стала поворотним моментом, який змусив світ переглянути свої пріоритети в міжнародних відносинах. Ця війна висвітлила низку гострих проблем, таких як безпека, суверенітет держав, демократія, права людини та ядерна безпека. Окремою серйозною загрозою є кіберзлочинність, яку Росія активно використовує для дестабілізації України та інших країн, для розвідки, шпигунства, підтримки військових операцій та поширення дезінформації [99].

Незважаючи на масштабні кібератаки російських зловмисників, спрямовані на підрив критичної інфраструктури та дестабілізацію ситуації в

Україні, українські фахівці з кібербезпеки продемонстрували стійкість та професіоналізм у відбитті цих загроз.

Тісна співпраця між державними органами, приватним сектором та міжнародними партнерами дозволила вчасно виявити та нейтралізувати кібератаки, мінімізувавши їх наслідки. Водночас, випадки успішного проникнення в системи критичної інфраструктури демонструють необхідність постійного вдосконалення стратегій кіберзахисту та розвитку експертизи в цій сфері.

Досвід протидії кібератакам з боку Росії став безцінним для України та міжнародної кібербезпекової спільноти, оскільки продемонстрував нові виклики та загрози, з якими держави можуть зіткнутися в майбутньому.

3.2 Перспективи розвитку кібербезпеки в Україні

Інформаційна безпека стала однією з найбільших проблем сучасного цифрового світу. Зі зростанням кількості кіберзлочинів та витонченості хакерських атак, підприємства та приватні особи стикаються з постійною загрозою порушення конфіденційності даних, втрати критично важливої інформації та фінансових втрат. Про інформаційну безпеку йдеться у Законі України «Про засади інформаційної безпеки України» [51]. У цьому нормативному акті термін «інформаційна безпека» трактується як захищеність найважливіших інтересів особи, суспільства і держави від потенційних загроз, пов’язаних з інформацією. Це включає захист від шкоди внаслідок неповноти, несвоєчасності або недостовірності інформації, порушення цілісності та доступності даних, несанкціонованого поширення конфіденційної інформації, негативного інформаційно-психологічного впливу, а також навмисного заподіяння шкоди внаслідок використання інформаційних технологій. Іншими словами, інформаційна безпека забезпечує надійність, автентичність та належний контроль доступу до інформації, яка є важливою для громадян, суспільства та країни в цілому.

Основними цілями державної політики з питань інформаційної безпеки є захист інформаційного суверенітету, збереження духовних і культурних цінностей українців, розвиток національної самоідентичності та цивілізаційної єдності, створення розвиненого інформаційного суспільства та інформаційного простору в Україні, перетворення країни в інформаційно розвинену державу та повноцінне членство в європейській та міжнародній спільноті.

Доктрина інформаційної безпеки України, Закон України «Про основи національної безпеки України», цей і інші закони України, такі як Закон України «Про інформацію», Закон України «Про захист персональних даних», Закон України «Про доступ до публічної інформації» та міжнародні договори, які Верховна Рада України схвалила, і інші нормативно-правові акти, які були видані на виконання законів, складають основу інформаційної безпеки.

Кібертероризм є однією з найсерйозніших загроз сучасності, що створює ризики для національної інформаційної безпеки, економічного розвитку та добробуту громадян. Терористичні угруповання та радикальні елементи все активніше використовують кіберпростір для пропаганди, фінансування, вербування нових членів, а також для здійснення прямих атак на критичну інфраструктуру, інформаційні системи та ресурси. Наслідки успішних кібертерактів можуть бути катастрофічними, призводячи до порушення функціонування життєво важливих об’єктів, витоку конфіденційних даних, дестабілізації економіки та навіть людських жертв.

Україна, на жаль, безпосередньо зіткнулася з цією загрозою під час російської агресії, коли кібератаки використовувались як невід’ємна складова гібридної війни. Хакерські угруповання на замовлення спецслужб РФ організовували масштабні атаки на державні установи, енергетичні системи, банківський сектор та інші критично важливі об'єкти України. Успішне відбиття цих атак продемонструвало необхідність посилення національного потенціалу кіберзахисту.

Але незважаючи на численні виклики та загрози кібертероризму, Україна має вагомі переваги, які необхідно повною мірою задіяти. Наявність команди

реагування на комп’ютерні надзвичайні події (CERT-UA), безцінний досвід протидії масштабним атакам під час російської агресії, високий рівень кваліфікованих вітчизняних ІТ-фахівців та існуюча нормативно-правова база у вигляді відповідних законів – усе це створює міцний фундамент для посилення протидії кібертероризму та виступає сильною стороною у кіберсфері України.

Крім того, Україна має низку перспективних можливостей, які варто використати, зокрема залучення додаткового міжнародного фінансування, технічної допомоги та впровадження новітніх технологій захисту на кшталт штучного інтелекту чи блокчейну, підвищення стійкості критичної інфраструктури, а також розбудова освітніх програм для підготовки фахівців із кібербезпеки.

Водночас, необхідно критично оцінювати нові виклики, серед яких – постійні кібератаки з боку Росії та її союзників, поява дедалі витонченіших векторів атак, загроза витоку даних через шпигунську діяльність інших держав, а також вразливість об’єктів критичної інфраструктури до кібертерористичних акцій та існуючі суттєві слабкі сторони, такі як застаріла ІТ-інфраструктура та системи в державних установах, недостатнє фінансування сфери кібербезпеки, нестача кваліфікованих кадрів у регіонах та низький рівень кібергігієни серед населення.

Лише максимально консолідувавши наявний потенціал та ресурси, Україна зможе випередити кіберзагрози та забезпечити надійний кіберзахист держави, бізнесу та громадян від терористичних посягань у цифровому просторі. Цей шлях вимагатиме узгоджених зусиль на всіх рівнях – від правових ініціатив до операційної взаємодії і технологічної модернізації систем захисту (Додаток А).

Щоб подолати критичний стан у сфері кібербезпеки, Україна має виробити комплексну стратегію із залученням усіх наявних ресурсів та можливостей. Це включає максимальне використання ефективної системи реагування на кіберінциденти CERT-UA, досвіду протидії масштабним

кібератакам, високого рівня кваліфікованих ІТ-фахівців та наявної стратегії кібербезпеки.

Водночас необхідно активно залучати додаткове фінансування, міжнародну технічну допомогу та інвестиції у модернізацію інфраструктури й інноваційні технології кібербезпеки.

Неможливо ігнорувати вразливість критичної інфраструктури, тому потрібно працювати над адаптацією передового досвіду й новітніх рішень для її захисту. І найголовніше – це розвиток кадрового потенціалу через масштабні освітні програми для підготовки та перекваліфікації фахівців з кібербезпеки як у великих містах, так і в регіонах. Лише комплексні скоординовані зусилля з реалізації цієї стратегії за активної участі всіх заінтересованих сторін зможуть суттєво зміцнити кібербезпеку України.

Ефективна система реагування на кіберінциденти CERT-UA є ключовим активом у протидії постійним кібератакам з боку Росії та її союзників. Посилення спроможностей CERT-UA шляхом залучення додаткових ресурсів та кваліфікованих кадрів дозволить швидко виявляти та блокувати атаки, розробляти дієві стратегії кіберзахисту на основі аналізу тактики супротивника. Крім того, розвинена мережа CERT-UA забезпечить оперативне розслідування інцидентів шпигунства та витоків даних в інтересах інших держав.

Наявний досвід протидії масштабним кібератакам під час російської агресії стане у нагоді для розробки контрзаходів проти нових витончених кіберзагроз та векторів атак. Ретельний аналіз попередніх інцидентів допоможе виявити слабкі місця, передбачити можливі майбутні сценарії та розробити проактивні стратегії захисту. Цей безцінний досвід також буде використано для створення ефективних механізмів убезпечення критичної інфраструктури.

Високий рівень кваліфікованих ІТ-спеціалістів в Україні дає змогу формувати потужні об’єднані групи для реагування на атаки, проведення досліджень нових загроз та розробки інноваційних рішень кіберзахисту. Провідних українських експертів варто залучати до проєктів зі створення спеціалізованих систем захисту критичної інфраструктури, а також

організовувати програми стажування та обміну досвідом з партнерами з НАТО для навчання персоналу протистояти сучасним викликам.

Наявність актуальної Стратегії кібербезпеки та відповідного законодавства дозволяє оперативно переглядати та вдосконалювати нормативні акти відповідно до нових загроз. Посилені вимоги до захисту критичної інфраструктури, державних систем та безпеки даних стануть на заваді шпигунству, витокам інформації та допоможуть убезпечити вразливі об'єкти від руйнівних кібератак.

Розглядаючи можливості у сфері кібербезпеки України, можна сказати, що залучення додаткового міжнародного фінансування та технічної допомоги допоможе подолати недоліки застарілої інфраструктури та систем в держустановах шляхом розробки цільових програм модернізації ІТ-інфраструктури. Це також дозволить вирішити проблему недостатнього фінансування сфери кібербезпеки через ініціювання спеціальних програм співпраці з міжнародними організаціями і розробку інвестиційних проектів для залучення грантів та кредитів від країн-партнерів. Нестача кваліфікованих кадрів у регіонах може бути подолана за рахунок спільних проектів міжнародних партнерів щодо підготовки фахівців у регіонах.

Впровадження новітніх технологій кіберзахисту, таких як штучний інтелект, блокчейн та аналітика великих даних, стане потужним інструментом для модернізації застарілих ІТ-систем та інфраструктури державних установ. Використання хмарних сервісів кіберзахисту дозволить зменшити навантаження на ці застарілі системи. Технології штучного інтелекту, аналітики даних та дистанційного навчання можуть бути ефективно застосовані для підготовки фахівців у регіонах та автоматизації процесів кіберзахисту. Штучний інтелект та машинне навчання також можуть використовуватись для виявлення загроз, спричинених людським фактором, підвищуючи рівень кібергігієни серед населення.

Підвищення рівня кібербезпеки критичної інфраструктури є пріоритетним завданням, яке допоможе вирішити проблему застарілих систем

державних установ. При цьому, зважаючи на обмежене фінансування, слід зосередити наявні ресурси на захисті найбільш критичних та вразливих об’єктів інфраструктури. Для регіонів важливо створити підрозділи кіберзахисту на базі критичної інфраструктури, а також проводити регулярні тренінги та підвищувати кваліфікацію персоналу цих об'єктів для посилення кібербезпеки.

Розвиток освітніх програм та центрів підготовки фахівців з кібербезпеки дозволить вирішити проблему нестачі кваліфікованих кадрів у регіонах шляхом створення мережі сертифікованих регіональних центрів кваліфікації. Для підвищення рівня кібергігієни серед населення необхідно запровадити обов’язкові курси з основ кібергігієни у школах та університетах, а також залучати волонтерів та студентів IT-спеціальностей для навчання громадян.

У матриці SWOT-аналізу представлено комплексний підхід до подолання слабких сторін та загроз кібербезпеці України. Для протидії кібератакам з боку Росії та новим загрозам необхідна модернізація інфраструктури: заміна застарілого обладнання, програмного забезпечення та впровадження новітніх технологій кібербезпеки. Для вирішення проблеми недостатнього фінансування галузі потрібно збільшити бюджетні видатки, залучити міжнародні кошти та інвестиції приватного сектору.

Нестачу кваліфікованих кадрів у регіонах планується подолати через створення спеціалізованих освітніх програм, надання стипендій, підтримку студентів, сприяння мобільності фахівців. Низький рівень кібергігієни населення має покращитися шляхом інформаційних кампаній та навчання безпечного користування інтернетом. Для захисту від шпигунства, витоків даних, загроз критичній інфраструктурі необхідна модернізація систем, створення резервних копій, регулярні аудити безпеки, публічно-приватне партнерство та інструменти виявлення таких загроз.

Перспективи розвитку кіберзахисту України є значними та обіцяють суттєві покращення у найближчі роки. Кіберзагрози, що стають все більш складними та витонченими, змушують Україну приділяти особливу увагу захисту своїх інформаційних систем.

Аналізуючи результати SWOT-аналізу та матриць подолання критичного стану, можна виокремити ключові вектори розвитку кіберзахисту України, які сприятимуть підвищенню стійкості до кіберзагроз і забезпеченню належного рівня кібербезпеки в державі.

По-перше, важливою є інтенсифікація міжнародного співробітництва задля залучення додаткового фінансування, технічної допомоги та обміну передовим досвідом. Співпраця з провідними організаціями, такими як НАТО, ЄС та ООН, у рамках Угоди про асоціацію з ЄС може стати потужним каталізатором модернізації застарілої інфраструктури, підвищення кваліфікації персоналу та впровадження інноваційних технологій кібербезпеки.

По-друге, імплементація новітніх технологій, зокрема штучного інтелекту, аналітики великих даних, хмарних сервісів та блокчейну, забезпечить підвищення ефективності виявлення та нейтралізації кіберзагроз. Ці рішення дозволять здійснювати проактивний захист від нових векторів атак, оперативно реагувати на інциденти та оптимізувати використання наявних ресурсів.

По-третє, вкрай важливим є посилення захисту критичної інфраструктури та державних ІТ-систем шляхом модернізації та впровадження спеціалізованих рішень кіберзахисту. Інвестування у безпеку об’єктів, пов’язаних з обслуговуванням населення, є запорукою забезпечення стійкості та безперервності надання життєво важливих послуг.

По-четверте, розбудова ефективної системи підготовки та перекваліфікації кадрів у сфері кібербезпеки сприятиме вирішенню проблеми дефіциту фахівців. Створення мережі регіональних центрів навчання, залучення провідних експертів, упровадження дистанційних форм та співпраця з міжнародними партнерами дозволять підвищити загальний рівень кваліфікації персоналу.

Нарешті, підвищення рівня кібергігієни серед населення через інформаційні кампанії, навчання основам безпеки в Інтернеті та залучення волонтерів і студентів ІТ-спеціальностей допоможе мінімізувати ризики,

пов’язані з людським фактором і недостатньою обізнаністю громадян про кіберзагрози [95].

Комплексна реалізація цих ключових векторів дозволить Україні суттєво посилити свої спроможності у сфері кіберзахисту, забезпечити стійкість критичної інфраструктури та державних систем до кібератак, а також підвищити рівень кібербезпеки в масштабах усієї держави

ВИСНОВКИ

У сучасну епоху інформаційний простір став потужним інструментом впливу на всі сфери життєдіяльності держави та суспільства. Національний інформаційний простір має вирішальне значення для забезпечення державного суверенітету, економічного розвитку, безпеки та формування громадянського суспільства. Він включає інформаційні ресурси, інфраструктуру, суб'єктів, які створюють і поширюють інформацію, та відповідне законодавче регулювання.

Інформаційний простір України зазнав значної еволюції, пройшовши шлях від радянської цензури до свободи слова та незалежності ЗМІ. Однак його розвиток не був легким, оскільки в умовах кризи та зовнішньої агресії національний інформаційний простір зіткнувся з серйозними викликами у вигляді дезінформації, пропаганди, кібератак та втручання з боку агресивних сил.

Ключовими рисами національного інформаційного простору є відкритість і свобода слова, постійна модернізація технологічної інфраструктури, забезпечення інформаційного суверенітету та безпеки держави. Досягнення балансу між демократичними свободами та надійним захистом від загроз є пріоритетним завданням.

На сучасному етапі Україна вживає комплексних заходів для зміцнення інформаційної безпеки, протидії дезінформації та кібератакам, посилення координації між органами влади та міжнародного співробітництва у цій сфері. Забезпечення стійкості національного інформаційного простору, підвищення медіаграмотності населення та інтеграція у світовий інформаційний простір визначають вектор подальшого розвитку.

Забезпечення належного рівня інформаційної безпеки є пріоритетом для провідних країн світу. Так, на приклад, США мають розгалужену систему відповідних відомств та значні ресурси для протидії кіберзагрозам. Франція реалізує комплексну національну програму цифрової безпеки та розвиває

співпрацю з Україною у цій сфері. Німеччина посилює законодавчі вимоги щодо захисту даних та критичної інфраструктури.

На міжнародному рівні НАТО усвідомлює високий ризик кібератак і створює спеціальні структури для реагування та стримування. ОБСЄ сприяє зміцненню довіри між державами в інформаційному просторі. В ЄС діє Агентство ENISA, яке є провідним експертним центром з питань кібербезпеки в Європі. Таким чином, країни об'єднують зусилля для протидії транснаціональним кіберзагрозам в умовах зростаючої глобалізації та диджиталізації.

На початку повномаштабного вторгнення Україна зазнала численних кібератак з боку Росії та підконтрольних їй хакерських угруповань. Статистика свідчить про значне зростання кількості кіберінцидентів порівняно з довоєнним періодом. Основними цілями атак стали об'єкти критичної інфраструктури, фінансові установи, державні органи та медіа-ресурси. Незважаючи на масштабність атак, система кібербезпеки України демонструє стійкість і здатність виявляти та нейтралізувати загрози завдяки професіоналізму фахівців та співпраці з міжнародними партнерами.

Підвищення ефективності кіберзахисту в Україні потребує комплексного підходу. Відповідно на державному рівні необхідно:

– По-перше, впровадити новітні технології, зокрема штучного інтелекту, аналітики великих даних, хмарних сервісів та блокчейну, що забезпечить проактивний захист від нових векторів атак та оптимізує використання наявних ресурсів.

– По-друге, посилити захист критичної інфраструктури та державних ІТ-систем шляхом їх модернізації та впровадження спеціалізованих рішень кібербезпеки, що гарантуватиме безперервність надання життєво важливих послуг.

– По-третє, розбудова ефективної системи підготовки та перекваліфікації кадрів у сфері кібербезпеки, створення регіональних центрів навчання та співпраця з міжнародними партнерами допоможуть вирішити проблему

дефіциту фахівців. Нарешті, підвищення рівня кібергігієни серед населення через інформаційні кампанії та залучення волонтерів і студентів IT-спеціальностей мінімізує ризики, пов’язані з людським фактором.

Комплексна реалізація цих ключових векторів забезпечить стійкість державних систем до кібератак та підвищить загальний рівень кібербезпеки в Україні.

Безпека кіберпростору є ключовим елементом національної безпеки в епоху цифрової трансформації. Лише завдяки системному та комплексному підходу можна ефективно протидіяти новітнім кіберзагрозам та забезпечити сталий розвиток держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стасюк Ю. М. Моделі міжнародного трансферу технологій. *Вісник ДНУ. Серія: світове господарство і міжнародні економічні відносини*. 2012. №. 4. С. 217-225. (дата звернення: 11.03.2024).

2. Фуркшев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // *Інформація і право*. №2 (5). 2012. С. 162-175. URL : https://ippi.org.ua/sites/default/files/12fvmsvv.pdf (дата звернення: 11.03.2024).

3. Солодка О.М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету // *Інформація і право*. № 4(35) /2020 С. 39-46. URL: file:///C:/Users/Admin/Downloads/221216.pdf (дата звернення: 11.03.2024).

4. Дубняк К.А. Інформаційний простір: структура та функціональні параметри // *Соціальні комунікації*. 2015 р., № 4 (24). С. 21–25. URL: http://umo.edu.ua/images/content/aspirantura/zabezp_discipl/Інформац.%20простір.pdf. (дата звернення: 11.03.2024).

5. Всесвітня мережа: Google створив дудл з нагоди її 30-річчя / 24 техно. 12.03.2019.URL:https://24tv.ua/tech/vsesvitnya_pavutina_30_rokiv_shho_tse_ta_chomu_google_stvoriv_dudl_n1125086. (дата звернення: 12.03.2024).

6. Даніч В.М, Шевченко С.М. Інформаційний простір // *Review of transport economics and management*, 2022, Iss. 8(24). С. 120–140. URL: https://typeset.io/pdf/information-space-2cgmnqbl.pdf. (дата звернення: 12.03.2024).

7. Слюсаревський М.М. Інформаційний простір: критика існуючих визначенні спроба побудови теорії. // Харківський держ. Ун-т. Вісник. Серія «Психологія, політологія»: Особистість і трансформаційні процеси у суспільстві». Харків, 1999. N 439. Ч. 4, 5. С. 337–342.

8. Токар О. Державна інформаційна політика: проблеми визначення концепту // Політичний менеджмент. 2009 № 5 С.131-141 URL:

https://ipiend.gov.ua/wp-content/uploads/2018/08/tokar_derzhavna.pdf (дата звернення: 11.03.2024).

9. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні // *Науковий вісник: Державне управління*, 2023. №1 (13), С. 195-210. URL: https://nvdu.undicz.org.ua/index.php/nvdu/ (дата звернення: 12.03.2024).

10. Солодка О.М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. // Інформація і право. 2020. №4 (35). С. 39-46 URL: https://ippi.org.ua/sites/default/files/5_19.pdf (дата звернення: 12.03.2024).

11. Добровольська А.Б. Інформаційний простір: проблеми становлення нової якості національного росту // *Наука України у світовому інформаційному просторі*. 2010. С. 61-71. URL: https://www.nas.gov.ua/publications/books/series/ (дата звернення: 12.03.2024).

12. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс // *Інформація і право*. № 1(32)/2020. С. 80-87. URL: https://ippi.org.ua/sites/default/files/9_15.pdf (дата звернення: 12.03.2024).

13. Нестеряк В.Ю. Становлення національного інформаційного простору України (період 1989–1993 років) // *Вісник НАДУ при Президентові України* (Серія «Державне управління») 2018. С. 11–17. URL: file:///C:/Users/Admin/Downloads/vnaddy_2018_1_4%20(1).pdf (дата звернення: 12.03.2024).

14. Про пресу та інші засоби масової інформації: Закон СРСР від 12.06.1990№1553.Відом.Верхов.РадиУкраїни. 1990. №26 .Ст. 492.

15. Про департизацію державних органів, установ та організацій: Постанова Верхов. Ради України від 24.08.1991 № 1429-XII. URL: http:// zakon2.rada.gov.ua/laws/show/1429-12 (дата звернення: 12.03.2024).

16. Інформаційне законодавство України : станом на 1 верес. 2008 р. / за ред. Т. Шевченка, Т. Олексіюк ; упоряд. Т. Бондаренко. Київ, 2008. 356 с

17. Про заборону діяльності Компартії України : Указ Президії Верховної Ради України від 30.08.1991 № 1468-XII. База даних «Законодавство

України» / ВР України. URL: http://zakon4.rada.gov. Ua/laws/show/1468-12 (дата звернення: 13.03.2024).

18. Інформація про зареєстровані періодичні видання : станом на 31 груд. 1991 р. / Держ. комітет України по пресі. – Київ, 1993.

19. Нестеряк Ю. В., Нестеряк Ю. М. Національний інформаційний простір України: трансформації (1989–2019 роки) : монографія. Київ : КНУ, 2021. 176 с.

20. Губерський Л. В. Інформаційна політика України: європейський контекст / Л. В. Губерський , Є. Є. Камінський, Є. А. Макаренко, М. А. Ожеван, О. І. Шнирков. – К. : Либідь, 2007. – 360 с.

21. Лазарчук О. Перспективи і сучасний стан ділового сегменту медіаринку України // *Вісник Львівського університету : зб. Наук. Пр. Серія Журналістика*. 2013. Вип. 38. С. 159–167.

22. Пояснювальна записка до проекту Закону України «Про засади інформаційної безпеки України». URL: http://w1.c1.rada.gov.ua/ pls/zweb2/webproc4_ 1?Pf3511=51123 (дата звернення: 15.03.2024).

23. Телепровайдер «Ланет» припиняє трансляцію «РТР», «Первого канала» та «НТВ» за антиукраїнську пропаганду // Урядовий кур’єр 04.03.2014 URL: https://ukurier.gov.ua/uk/news/teleprovajder-lanet-pripinyaye-translyaciyu-rtr-pe/ (дата звернення: 15.03.2024).

24. Боднар І.Р. Інформаційна безпека як основа національної безпеки // *Механізм регулювання економіки*. 2014. № 1. С.68-75. URL: https://core.ac.uk/download/pdf/141443493.pdf (дата звернення: 16.03.2024).

25. Питання діяльності Міністерства інформаційної політики України : Постанова Каб. Міністрів України від 14.01.2015 № 2. URL: http:// zakon4.rada.gov.ua/laws/show/2-2015- %D0 %BF (дата звернення: 16.03.2024).

26. Brzezinski Zbigniew. Receives Jury du Prix Tocqueville Prize October 14, 2011. URL: csis.org/analysis/ zbigniew-brzezinski-receives-jury-du-prix-tocquevilleprize (дата звернення: 16.03.2024).

27. Петрик В.П. Сутність інформаційної безпеки держави, суспільства та особи // Юстініан. 2009. С. 122–135.

28. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.

29. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : указ Президента України №47/2017. URL: https://www.president.gov.ua/documents/472017 (дата звернення: 18.03.2024).

30. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України. URL: http://www.dsaua.org/index. Php?Option=com_content&view=article&id=198%3A2014-08 (дата звернення: 18.03.2024).

31. Ільницька У. Інформаційна безпека україни: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам // *Політичні науки*. С. 27–32. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf. (дата звернення: 20.03.2024).

32. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Рішення Ради нац. безпеки і оборони України від 28.04.2014 р. : станом на 1 трав. 2014 р. URL: https://zakon.rada.gov.ua/laws/show/n0004525-14#Text (дата звернення: 20.03.2024).

33. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози // *Вісник Харківського національного університету імені В.Н. Каразіна*, серія «Питання політології» 42: 50-57. URL: https://doi.org/10.26565/2220-8089-2022-42-08 (дата звернення: 22.03.2024).

34. Про виділення коштів з резервного фонду державного бюджету щодо забезпечення інформаційної безпеки та захисту інформаційного простору

держави : Розпорядж. Каб. Міністрів України від 07.05.2022 р. № 366-р. URL: https://zakon.rada.gov.ua/laws/show/366-2022-%D1%80#Text (дата звернення: 22.03.2024).

35. Про утворення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави : Постанова Каб. Міністрів України від 08.03.2024 р. № 276. URL: https://zakon.rada.gov.ua/laws/show/276-2024-%D0%BF#n9 (дата звернення: 22.03.2024).

36. Age of Cybercrime: Global. URL: https://www.linkedin.com/pulse/age-cybercrime-global-crawsec-z1kwf (дата звернення: 02.04.2024).

37. Profiling a Cyber Criminal // Міжнародний журнал телекомунікацій і нових технологій. 2021. Т.2 №7 URL : https://www.ripublication.com/irph/ij.pdf (дата звернення: 02.04.2024).

38. Cybercrime. // Oxford English Dictionary URL: https://www.oed.com/search/dictionary/?scope=Entries&q=cybercrime (дата звернення: 02.04.2024).

39. Cyber crime. // Oxford English Dictionary URL: https://www.naavi.org/pati/pati_cybercrimes_dec03.htm (дата звернення: 05.04.2024).

40. Cyber crime and its classification. // Oxford English Dictionary URL: https://www.bbau.ac.in/dept/Law/TM/1.pdf (дата звернення: 05.04.2024).

41. Харитоненко І.О. Феномен кіберзлочинності в сучасній кримінологічній теорії // Кримінальне право та кримінологія. 2020. С. 401–404. URL:file:///C:/Users/Admin/Downloads/ (дата звернення: 05.04.2024).

42. Кібербулінг: що це, яким він буває та як від нього захистити свою дитину // телеграф. 21.11.2019 URL: https://www.telegraf.in.ua/kremenchug/10082081-kberbulng-scho-ce-yakim-vn-buvaye-ta-yak-vd-nogo-zahistiti-svoyu-ditinu.html (дата звернення: 05.04.2024).

43. What Is Cyberbullying. URL: https://www.stopbullying.gov/cyberbullying/what-is-it (дата звернення: 07.04.2024).

44. What is a phishing attack? URL: https://www.cloudflare.com/learning/access-management/phishing-attack/ (дата звернення: 07.04.2024).

45. What is a DDoS Attack? – DDoS Meaning. URL: https://www.kaspersky.com/resource-center/threats/ddos-attacks (дата звернення: 10.04.2024).

46. What is Salami Attack? URL:https://www.geeksforgeeks.org/what-is-salami-attack/ (дата звернення: 10.04.2024).

47. Malware Attacks: Definition and Best Practices. URL:https://www.rapid7.com/fundamentals/malware-attacks/ (дата звернення: 13.04.2024).

48. What is cyberterrorism? URL:https://www.techtarget.com/searchsecurity/definition/cyberterrorism (дата звернення: 13.04.2024).

49. What Is Cyber Warfare? URL:https://www.fortinet.com/lat/resources/cyberglossary/cyber-warfare (дата звернення: 13.04.2024).

50. ЗайцеваКалаурІ.В. Міжнародна інформаційна безпека. Міжнародна інформаційна безпека // *IV Міжнародна студентська наукова конференція «Правова система України в умовах європейської інтеграції: погляд студентської молоді».* 2020. С. 274 – 276. URL: http://dspace.wunu.edu.ua/bitstream/316497/40666/1/274.pdf (дата звернення: 13.04.2024).

51. Про засади інформаційної безпеки України : Проект Закону України від 28.05.2014 р. № 4949. URL: https://ips.ligazakon.net/document/J. (дата звернення: 14.04.2024).

52. What is Information Security (InfoSec)? URL: https://www.imperva.com/learn/data-security/information-security-infosec/ (дата звернення: 17.04.2024).

53. NATO: Time to Adopt a Pre-emptive Approach to Cyber Security in New Age Security Architecture. URL: https://gjia.georgetown.edu/2024/03/09/nato-time-to-adopt-a-pre-emptive-approach-to-cyber-security-in-new-age-security-architecture/ (дата звернення: 17.04.2024).

54. Cyber defence. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 19.04.2024).

55. Cyber/ICT Security. URL: https://www.osce.org/cyber-ict-security (дата звернення: 19.04.2024).

56. European Network and Information Security Agency (ENISA). URL: https://www.europeansources.info/record/european-network-and-information-security-agency-enisa/ (дата звернення: 20.04.2024).

57. European Union Agency for Cybersecu. URL:https://dig.watch/actor/european-union-agency-network-and-information-security (дата звернення: 20.04.2024).

58. Білоусов О.С., Татакі Д.Д., Татакі О.О. Міжнародна інформаційна безпека в США // Філософія та політологія в контексті сучасної культури. 2023. Т.15. No 2. С. 82 – 89. URL: https://fip.dp.ua/index.php/FIP/article/view/1178/1313 (дата звернення: 20.04.2024).

59. Top Cybersecurity Laws and Regulations in France. URL: https://www.upguard.com/blog/cybersecurity-laws-regulations-france (дата звернення: 20.04.2024).

60. Cybersecurity Laws and Regulations in Germany. URL: https://www.upguard.com/blog/cybersecurity-laws-and-regulations-germany (дата звернення: 23.04.2024).

61. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV : станом на 8 лип. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 25.04.2024).

62. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 25.05.2024).

63. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017 : станом на 30 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 25.05.2024).

64. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 25.05.2024).

65. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017 : станом на 30 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 25.05.2024).

66. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» : Указ Президента України від 14.03.2016 р. № 92/2016 : станом на 27 берез. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/92/2016#Text (дата звернення: 25.05.2024).

67. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.05.2024).

68. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента

України від 26. 08. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/showText (дата звернення: 25.05.2024).

69. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // *Ресурсний центр ГУРТ*. 3.10.2016 URL: https://www.gurt.org.ua/articles/34602/ (дата звернення: 26.04.2024).

70. Голіна В.В., Головкін Б.М. Кримінологія: загальна та особлива частини: навч. посіб. Харків: Право, 2014. 513 с

71. About CISA. URL: https://www.cisa.gov/about (дата звернення: 26.04.2024).

72. Significant Cyber Incidents. URL: https://www.csis.org/programs/-cyber-incidents (дата звернення: 26.04.2024).

73. NSA Publishes 2023 Cybersecurity Year in Review. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3621654/nsa-publishes-2023-cybersecurity-year-in-review/ (дата звернення: 26.04.2024).

74. Cyber Attacks Reveal Uncomfortable Truths About U.S. Defenses. URL: https://www.rand.org/pubs/commentary/2023/09/cyber-attacks-reveal-uncomfortable-truths-about-us.html (дата звернення: 26.04.2024).

75. Ransomware attacks on US government organizations have cost over $860m. URL: https://www.comparitech.com/blog/information-security/government-ransomware-attacks/ (дата звернення: 27.04.2024).

76. Угода про співробітництво у сфері безпеки між Україною та Францією // *Офіційне інтернет представництво. Президент України*. 16.02.2024. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89005 (дата звернення: 27.04.2024).

77. NATO steps up intelligence-sharing ‘in preparation’ for Russian cyberattacks.URL: https://www.politico.eu/article/nato-steps-up-intelligence-sharing-in-preparation-of-russian-cyberattacks/ (дата звернення: 27.04.2024).

78. NATO establishes program to coordinate rapid response to cyberattacks. URL: https://www.politico.com/news/2022/06/29/nato-cyberattacks-russia-00043149 (дата звернення: 27.04.2024).

79. Дефейс. // Словотвір. URL: https://slovotvir.org.ua/words/defeis (дата звернення: 30.04.2024).

80. Шевченко Л.. Хакери змогли зламати 70 урядових сайтів, зокрема сайт «Дії». Як це вдалося? // Детектор медіа. 14.01.2022. URL: https://tech.liga.net/ua/ukraine/article/kak-hakery-smogli-vzlomat-70-pravitelstvennyh-saytov-i-kto-za-etim-mojet-stoyat (дата звернення: 28.04.2024).

81. Що відомо про DDoS-атаку на держсайти та банки: пік до 150 Гбіт/с, ймовірно з РФ // ain. 19.02.2022 URL: https://ain.ua/2022/02/16/shho-vidomo-pro-ddos-ataku-15-lut/ (дата звернення: 28.04.2024).

82. Юрасов С. Ніякої «найпотужнішої кібератаки в історії України» не було». Інтернет-бізнесмени тролять Мінцифри і Міноборони // dev.ua. 17.02.2022URL: https://web.archive.org/web/20220218001113/https://dev.ua/news/not-a-big-deal-attack (дата звернення: 28.04.2024).

83. Сайти банків та органів влади зазнали масової DDoS-атаки // УКРІНФОРМ. 23.02.2022. URL: https://www.ukrinform.ua/rubric-technology/3410542-sajti-bankiv-ta-organiv-vladi-zaznali-masovoi-ddosataki.html (дата звернення: 01.05.2024).

84. HermeticWiper: New data-wiping malware hits Ukraine. URL: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/ (дата звернення: 01.05.2024).

85. Сайт Київської ОДА атакують хакери. // УКРІНФОРМ. 24.02.2024.URL: https://www.ukrinform.ua/rubric-technology/3411812-sajt-kiivskoi-oda-atakuut-hakeri.html (дата звернення: 01.05.2024).

86. Email-адреси українських військових атакують хакери. // УКРІНФОРМ. 25.02.2024. URL: https://www.ukrinform.ua/rubric-technology/3412829-emailadresi-ukrainskih-vijskovih-atakuut-hakeri.html (дата звернення: 01.05.2024).

87. Звіт за другий квартал 2023. // Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. 20.07.2023. URL: https://scpc.gov.ua/uk/articles/318 (дата звернення: 03.04.2024).

88. Звіт за третій квартал 2022 року. // Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk/articles/163 (дата звернення: 03.04.2024).

89. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики // Forbes. 04.05.2023 URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата звернення: 03.05.2024).

90. Звіт за перший квартал 2023. // Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. 15.04.2023. URL: https://scpc.gov.ua/uk/articles/306 (дата звернення: 05.05.2024).

91. Звіт за третій квартал 2023. // Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. 25.10.2023. URL: https://scpc.gov.ua/uk/articles/327 (дата звернення: 06.05.2024).

92. Звіт за четвертий квартал 2023. // Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. 31.01.2023. URL: https://scpc.gov.ua/uk/articles/341 (дата звернення: 06.05.2024).

93. Журавель Максим. Від 2024 року Кремль проти України буде збільшувати кількість кібератак зі штучним інтелектом // ТСН.06.12.2023 URL: https://tsn.ua/ato/v-2024-roci-kreml-proti-ukrayini-bude-zbilshuvati-kilkist-kiberatak-zi-shtuchnim-intelektom-2466091.html (дата звернення: 06.05.2024).

94. Ященко Т. Кіберзлочинність як нова форма ведення війни: виклики та шляхи протидії // Політ. Сучасні проблеми науки. Міжнародні відносини : Тези доп. XXV Міжнар. науково-практ. конф. здобувачів вищ. освіти і молодих уч., м. Київ, 2–5 квіт. 2024 р. С. 124–126.

95. Russian hackers strike French National Assembly website. URL: https://www.politico.eu/article/french-national-assembly-website-russian-cyberattack-hack-kremlin-emmanuel-macron/ (дата звернення: 29.05.2024).

96. Data Breaches and Cyber Attacks in Europe in March 2024 – 102,499,341 Records Breached. URL: https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-europe-in-march-2024-102499341-records-breached (дата звернення: 29.05.2024).

97. Data of half the population of France stolen in its largest ever cyberattack. URL: https://www.euronews.com/next/2024/02/08/data-of-33-million-people-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we (дата звернення: 29.05.2024).

98. Ященко Т. Кіберзлочинність як актуальна проблема сучасних міжнародних відносин // Дипломатія в міжнародних відносинах: сучасні виклики та перспективи : Матеріали Всеукр. науково-практ. конф. з міжнар. участю, м. Київ, 29 лют. 2024 р. 2024. С. 299.

99. Russian hackers launch cyberattack on Germany in Leopard retaliation. URL: https://www.euronews.com/2023/01/26/russian-hackers-launch-cyberattack-on-germany-in-leopard-retaliation (дата звернення: 29.05.2024).

100. The State of IT Security in Germany 2023. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf (дата звернення: 29.05.2024).

ДОДАТОК А

SWOT аналіз кібербезпеки України

Сильні сторони	**Слабкі сторони**
Ефективна система реагування на кіберінциденти (CERT-UA)	Застаріла інфраструктура та системи в держустановах
Досвід протидії масштабним кібератакам під час російської агресії	Недостатнє фінансування сфери кібербезпеки
Високий рівень кваліфікованих IT-спеціалістів	Нестача кваліфікованих кадрів у регіонах
Наявність Стратегії кібербезпеки та відповідних законів	Низький рівень кібергігієни серед населення

Можливості	**Загрози**
Залучення додаткового міжнародного фінансування та технічної допомоги	Постійні кібератаки з боку РФ та її союзників
Впровадження новітніх технологій кіберзахисту (ШІ, блокчейн тощо)	Нові витончені кіберзагрози та вектори атак
Підвищення рівня кібербезпеки критичної інфраструктури	Шпигунство та витік даних в інтересах інших держав
Розвиток освітніх програм та центрів підготовки фахівців з кібербезпеки	Вразливість критичної інфраструктури

ДОДАТОК В

Матриця подолання критичного стану

	Ефективна система реагування на кіберінциденти (CERT-UA)	Досвід протидії масштабним кібератакам під час російської агресії	Високий рівень кваліфікованих IT-спеціалістів	Наявність Стратегії кібербезпеки та відповідних законів
Залучення додаткового міжнародного фінансування та технічної допомоги	Використовувати наявні можливості CERT-UA для залучення міжнародного фінансування та допомоги, щоб розширити свої можливості та підвищити ефективність.	Додаткове фінансування може бути використано для вдосконалення інфраструктури кібербезпеки України, включаючи закупівлю нового обладнання та програмного забезпечення. Також міжнародна допомога може стимулювати дослідження та розробки нових технологій та методів протидії кіберзагрозам.	Додаткове фінансування може бути використано для надання стипендій та грантів студентам та фахівцям з кібербезпеки.	Міжнародні експерти можуть допомогти удосконалити існуючі закони та нормативні акти, враховуючи глобальні тенденції та найкращі практики у сфері кібербезпеки. Це забезпечить більш ефективне регулювання та контроль у цій галузі.
Впровадження новітніх технологій кіберзахисту (ШІ, блокчейн тощо)	ШІ може допомогти CERT-UA автоматизувати аналіз даних про кіберзагрози, що дозволить швидше виявляти та реагувати на кібератаки	ШІ може допомогти аналізувати дані про попередні кібератаки, що дозволить краще розуміти методи та тактику російських хакерів та розробляти	Використання новітніх технологій для автоматизації рутинних завдань з кібербезпеки, що звільнить час кваліфікованих IT-спеціалістів для вирішення більш складних	Можуть використовуватися для створення децентралізованої системи звітності про кіберінциденти, що допоможе уряду краще розуміти кіберзагрози та розробляти ефективніші політики

		ефективніші стратегії захисту	завдань.	кібербезпек
Підвищення рівня кібербезпеки критичної інфраструктури	Ефективна система реагування на кіберінциденти (CERT-UA) зможе бути повною мірою задіяна для виявлення, аналізу та нейтралізації кіберзагроз, що постають перед критичною інфраструктурою	Наявний досвід протидії масштабним кібератакам під час російської агресії дозволить краще підготуватися до захисту критично важливих об'єктів шляхом впровадження передових практик, технологій та оперативних процедур.	Високий рівень кваліфікованих IT-спеціалістів можна буде залучити до розробки комплексних систем кіберзахисту для об'єктів критичної інфраструктури. Їхня експертиза дозволить спроектувати надійні, гнучкі та ефективні рішення.	Стратегія кібербезпеки та відповідні закони створюють необхідне нормативно-правове підґрунтя для визначення вимог, стандартів і регуляторних норм щодо захисту критичної інфраструктури від кібератак
Розвиток освітніх програм та центрів підготовки фахівців з кібербезпеки	Розширення освітніх програм дозволить підготувати більше висококваліфікованих фахівців, які зможуть працювати в CERT-UA та посилити його спроможності	Цей досвід може бути інтегрований в освітні програми, щоб майбутні фахівці могли засвоїти уроки та передові практики захисту від подібних атак.	Існуючі висококласні IT-фахівці зможуть бути залучені як викладачі та менторами для підготовки нових кадрів у сфері кібербезпеки, передаючи свої знання та навички.	Розробка освітніх програм має базуватися на положеннях стратегії та нормативно-правової бази, щоб забезпечити відповідність підготовки фахівців актуальним вимогам та стандартам.

Матриця подолання критичного стану

	Ефективна система реагування на кіберінциденти (CERT-UA)	Досвід протидії масштабним кібератакам під час російської агресії	Високий рівень кваліфікованих IT-спеціалістів	Наявність Стратегії кібербезпеки та відповідних законів
Постійні кібератаки з боку РФ та її союзників	Посилення спроможностей CERT-UA шляхом залучення додаткових ресурсів та висококваліфікованих фахівців	Провести ретельний аналіз тактики та методів російських хакерів під час попередніх атак та розробити передові стратегії кіберзахисту на основі цього досвіду.	Створити об'єднані групи реагування з провідних українських IT-експертів. Залучити їх до розробки інноваційних рішень виявлення та блокування атак. Організувати програми стажування та обміну досвідом з експертами з країн НАТО.	Переглянути та посилити законодавство у сфері кібербезпеки. Ввести жорсткі вимоги до захисту критичної інфраструктури від кібератак. Активізувати міжнародне співробітництво в рамках Угоди про асоціацію з ЄС.
Нові витончені кіберзагрози та вектори атак	Посилити аналітичні спроможності CERT-UA для виявлення нових загроз та векторів атак та інтегрувати новітні інструменти моніторингу, штучний інтелект та аналітику великих даних	Розробити проактивні стратегії захисту від передбачуваних векторів атак Регулярно проводити спеціалізовані навчання для підтримки готовності до протидії новим загрозам	Створити спеціалізовані дослідницькі групи для вивчення нових кіберзагроз Залучити провідних експертів до розробки інноваційних рішень кіберзахисту Організувати програми підвищення кваліфікації для ознайомлення фахівців з останніми загрозами	Регулярно оновлювати Стратегію та нормативні акти відповідно до виявлених нових загроз Впроваджувати обов'язкові вимоги кіберзахисту для критичної інфраструктури та державних систем
Шпигунство та витік даних в інтересах інших держав	Розробити спеціальні процедури оперативного розслідування та блокування таких	Розробити контрзаходи та захисні механізми для уникнення подібних	Створити спеціалізовані групи для моніторингу та аналізу підозрілої	Запровадити чіткі вимоги до державних установ і критичної інфраструктури

	інцидентів	ситуацій Провести навчання для підвищення обізнаності персоналу щодо ризиків витоку даних	діяльності Організувати програми обміну досвідом з зарубіжними партнерами в протидії кібершпигунству	щодо безпеки даних
Вразливість критичної інфраструктури	Створити постійний канал обміну інформацією між CERT-UA та операторами критичних систем	Визначити основні вектори та методи, що застосовувалися хакерами Розробити ефективні захисні рішення та плани відновлення критичних систем на основі цього досвіду	Сформувати групи експертів для розробки спеціалізованих систем кіберзахисту критичної інфраструктури Залучити їх до проведення аудитів безпеки та усунення вразливостей	Затвердити обов'язкові стандарти та регуляторні норми захисту критично важливих об'єктів

Матриця подолання критичного стану

	Залучення додаткового міжнародного фінансування та технічної допомоги	Впровадження новітніх технологій кіберзахисту (ШІ, блокчейн тощо)	Підвищення рівня кібербезпеки критичної інфраструктури	Розвиток освітніх програм та центрів підготовки фахівців з кібербезпеки
Застаріла інфраструктура та системи в держустановах	Розробити цільові програми модернізації ІТ-інфраструктури державних установ	Запровадити системи захисту на основі штучного інтелекту, аналітики великих даних тощо Інтегрувати хмарні сервіси кіберзахисту для зменшення навантаження на застарілу інфраструктуру	Пріоритетно модернізувати ІТ-системи об'єктів критичної інфраструктури	Створити центри сертифікації персоналу держустанов з питань кібербезпеки Залучати випускників для оновлення систем та впровадження сучасних технологій
Недостатнє фінансування сфери кібербезпеки	Ініціювати спеціальні програми співпраці з міжнародними організаціями (НАТО, ЄС, ООН) у сфері кібербезпеки Розробити інвестиційні проєкти для залучення грантів, кредитів від країн-партнерів	Фокусуватися на більш економічно ефективних хмарних рішеннях кібербезпеки замість дорогого обладнання	Зосередити наявні ресурси на захисті найбільш критичних та вразливих об'єктів інфраструктури	Оптимізувати витрати на підготовку кадрів через дистанційні та змішані форми навчання
Нестача кваліфікованих кадрів у регіонах	Ініціювати спільні проєкти з міжнародними партнерами щодо підготовки кадрів у регіонах	Використовувати дистанційні форми навчання та віртуальні тренажери для підготовки фахівців у регіонах Залучати технології штучного інтелекту,	Створити регіональні підрозділи кіберзахисту на базі критичної інфраструктури	Створити мережу сертифікованих регіональних центрів підготовки та перекваліфікації кадрів

		аналітики даних для автоматизації процесів кіберзахисту		
Низький рівень кібергігієни серед населення	Ініціювати спеціальні освітні проєкти з підвищення кібергігієни за підтримки міжнародних організацій	Використовувати штучний інтелект та машинне навчання для виявлення загроз, спричинених людським фактором	Зосередити зусилля на захисті об'єктів критичної інфраструктури, пов'язаних з обслуговуванням населення Проводити регулярні тренінги та підвищувати кваліфікацію персоналу цих об'єктів	Запровадити обов'язкові курси з основ кібергігієни у школах та університетах Залучати волонтерів та студентів ІТ-спеціальностей для навчання громадян

Матриця подолання критичного стану

	Застаріла інфраструктура та системи в держустановах	Недостатнє фінансування сфери кібербезпеки	Нестача кваліфікованих кадрів у регіонах	Низький рівень кібергігієни серед населення
Постійні кібератаки з боку РФ та її союзників	Заміна застарілого обладнання та програмного забезпечення на сучасні аналоги. Впровадження нових технологій кібербезпеки	Виділення більше коштів для розвитку та підтримки ініціатив у галузі кібербезпеки. Це може бути здійснено через збільшення бюджетних призначень, а також заохочення приватного сектору до інвестування у цю сферу.	Для забезпечення належного рівня кібербезпеки необхідно навчати і підготовляти кваліфікованих кадрів. Уряд може розглядати створення програм навчання, підтримки студентів у галузі кібербезпеки та підвищення привабливості професії.	Проведення кампаній з просвітництва та навчання населення про кібербезпеку може значно покращити ситуацію. Це може включати інформаційні кампанії, тренінги та вебінари для широкої аудиторії.
Нові витончені кіберзагрози та вектори атак	Влада повинна приділити увагу модернізації систем інформаційної безпеки в державних установах. Це може включати оновлення апаратного забезпечення, програмного забезпечення та застосування сучасних методів шифрування та захисту даних.	Влада повинна виділити більше коштів на підтримку програм з кібербезпеки, які включають у себе інвестиції у розвиток нових технологій, тренування персоналу та розвиток кіберзахисту.	Для запобігання нестачі кваліфікованих кадрів у сфері кібербезпеки, важливо підтримувати освітні програми та навчання у галузі кібербезпеки. Можливі заходи включають створення спеціалізованих навчальних програм, стипендій та підтримки для студентів та молодих професіоналів.	Важливо проводити інформаційні кампанії щодо основних правил кібербезпеки серед населення. Це включає в себе заходи по навчанню користувачів безпечному використанню Інтернету, використанню надійних паролів, уникненню піратства програмного забезпечення та усвідомленню ризиків онлайн-шахрайства.

Шпигунство та витік даних в інтересах інших держав	Уряд повинен виділити достатні ресурси для модернізації інфраструктури та систем в держустановах, включаючи впровадження захисту від кібератак та оновлення програмного забезпечення до актуальних версій. Також варто стимулювати публічно-приватні партнерства для спільного фінансування цих проектів.	Уряд повинен збільшити бюджетне фінансування на заходи з підвищення кібербезпеки. Також можна розглянути можливість привернення інвестицій в цей сектор з боку приватного сектору шляхом створення спеціальних програм та стимулів.	Необхідно вдосконалювати систему підготовки та підвищення кваліфікації кадрів у сфері кібербезпеки. Це може включати створення спеціалізованих навчальних програм, організацію майстер-класів та тренінгів, а також підтримку участі фахівців у міжнародних конференціях та проектах.	Уряд повинен активно просувати програми з підвищення кібергігієни серед населення, включаючи проведення освітніх кампаній та розповсюдження інформації про основні правила безпеки в Інтернеті. Також важливо розвивати інструменти для виявлення та протидії шпигунству та витокам даних.
Вразливість критичної інфраструктури	Інвестування у оновлення та модернізацію існуючих систем та інфраструктури для забезпечення вищого рівня безпеки. Створення резервних копій даних. Регулярне створення та зберігання резервних копій даних для запобігання втраті інформації у випадку кібератак або випадкового знищення.	Надання фінансових стимулів (наприклад, податкові пільги або субсидії) для компаній, що інвестують у кібербезпеку.	Створення програм для стимулювання мобільності фахівців з кібербезпеки між регіонами та містами.	Проведення інформаційних кампаній з підвищення обізнаності населення щодо кібербезпеки та основних правил безпеки в Інтернеті. Проведення регулярних аудитів безпеки критичної інфраструктури та впровадження заходів для її захисту.