МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МІЖНАРОДНИХ ВІДНОСИН
ІМ. Б.Д. ГАВРИЛИШИНА
Кафедра міжнародних економічних відносин

ЛУЦІВ Ольга Сергіївна

КІБЕРБЕЗПЕКА ТА МІЖНАРОДНІ КОНФЛІКТИ: ВИКЛИКИ ТА МОЖЛИВІ СТРАТЕГІЇ

спеціальність: 292 Міжнародні економічні відносини
освітньо-професійна програма - Міжнародні економічні відносини

Кваліфікаційна робота

Виконав(ла) студент(ка)
групи МЕВ-41
ЛУЦІВ Ольга Сергіївна
_____
підпис
Науковий керівник:
к.е.н., доцент, О. М. Войтенко
_____
підпис

Кваліфікаційну роботу
допущено до захисту
«___»_____ 20__р.
Завідувач кафедри

_____
підпис

Тернопіль - 2024

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі, де цифрові технології відіграють ключову роль у функціонуванні всіх сфер суспільства, кібербезпека стає надзвичайно важливою складовою національної та міжнародної безпеки. Міжнародні конфлікти все частіше включають у себе кібероперації, які мають на меті завдати шкоди інформаційним системам держав, корпорацій та інфраструктури, що призводить до значних економічних, політичних та соціальних наслідків.

Дослідження викликів та можливих стратегій у сфері кібербезпеки в контексті міжнародних конфліктів є надзвичайно актуальним для формування ефективної політики безпеки та міжнародної співпраці. Це дозволить розробити дієві механізми захисту, зміцнити національні системи кібербезпеки та сприяти глобальній стабільності та безпеці у цифрову епоху.

Мета та завдання дослідження. Метою кваліфікаційної роботи є дослідження та аналіз впливу кібербезпеки на міжнародні конфлікти, визначення основних викликів, з якими стикаються держави та організації у сучасному кіберпросторі, Відповідно до поставленої мети визначимо наступні завдання:

- дослідити теоретичні засади трактування поняття «кібербезпека»;
- проаналізувати стан кібербезпеки країн в мовах міжнародних конфліктів
- провести аналіз впливу кібератак на кібербезпеку України в умовах військового конфлікту;
- запропонувати стратегію запобігання наслідкам кібератак.

Об'єктом дослідження є міжнародні конфлікти, що виникають у кіберпросторі, та їх вплив на безпеку держав, організацій та глобальну стабільність.

Предметом дослідження є виклики кібербезпеки, з якими стикаються держави та організації під час міжнародних конфліктів, а також можливі стратегії для підвищення рівня захисту та ефективної відповіді на кіберзагрози.

Методи дослідження. В кваліфікаційній роботі використовувалися такі методи як: методи емпіричного дослідження (спостереження, порівняння);

методи, використовувані для емпіричного та теоретичного досліджень (абстрагування, аналіз і синтез, індукція та дедукція, моделювання); методи теоретичного дослідження (ідеалізація, формалізація, гіпотеза та припущення, системний підхід).

Практичне значення одержаних результатів Результати даного дослідження мають важливе практичне значення для вдосконалення підходів до кібербезпеки в контексті міжнародних конфліктів. Зокрема, вони можуть бути використані для: **н**адання урядам та міжнародним організаціям рекомендацій щодо формування ефективних політик та стратегій для запобігання кіберзагрозам і реагування на них у контексті міжнародних конфліктів.

Апробація результатів дослідження. Основні аспекти і положення роботи доповідалися автором на XVII Міжнародній науково-практичній конференції молодих учених і студентів «Інноваційні процеси економічного і соціально-культурного розвитку: вітчизняний та зарубіжний досвід» (м. Тернопіль, 27–28 березня 2024 року) та тезисно опубліковані в матеріалах конференції.

Структура роботи. Кваліфікаційна робота складається з вступу, трьох розділів, висновків та списку використаних джерел. Робота вміщує 2 таблиці та 4 рисункs. Загальний обсяг кваліфікаційної роботи - 37 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ТРАКТУВАННЯ ПОНЯТТЯ «КІБЕРБЕЗПЕКА»

У вивченні захисту даних терміни «кібербезпека» та «інформаційна безпека» часто використовуються як синоніми. Із впровадженням нових технологій майже щодня та появою багатьох пов’язаних термінів не дивно, що точаться дискусії щодо єдності та відмінності цих термінів захисту даних.

Стрімкий розвиток мережевих та інформаційних технологій, який спостерігається в останнє десятиліття, створює умови для виникнення суттєвих змін у всіх сферах і галузях суспільного життя. Зростання ролі технологій неминуче призводить до виникнення ризиків, пов’язаних із забезпеченням цифрової безпеки інформації та вимагає своєчасного внесення необхідних коригувань її захисту. Тому система захисту інформації повинна постійно адаптуватися до нових умов, щоб забезпечити достатню безпеку як цифрової інформації, так і інформації, що зберігається на традиційних носіях.

Крім стандартних перетворень, пов'язаних з безпосереднім вдосконаленням технологій, система безпеки повинна швидко реагувати на несподівані зміни в результаті вимушених заходів. Проте багато хто не повністю готові до трансформації формату роботи через епідеміологічні обмеження, що призвело до появи додаткових загроз інформаційній безпеці (витік персональних даних, несанкціонований доступ третіх осіб, порушення правил захисту персональних даних).

В даний час середовище кібербезпеки є швидким, динамічним і постійно розвивається, тому система захисту комерційної компанії повинна постійно вдосконалюватися [1]. Великі й малі організації щодня піддаються атакам, починаючи від простих фішингових електронних листів і закінчуючи складними, витонченими операціями, організованими злочинними угрупованнями, і з кожною новою вразливістю готова скористатися новою. Впровадження кібербезпеки не обов’язково коштуватиме цілих грошей або займатиме багато часу. Незалежно від розміру комерційної компанії,

покращення кібербезпеки може допомогти захистити її власні дані та дані клієнтів, що зазвичай покращує ділові відносини та відкриває нові можливості для бізнесу. Кібербезпека стає критично важливою складовою успіху бізнесу та найважливішим захистом від загроз інформаційної ери.

Хакерство, фішинг і зловмисне програмне забезпечення зараз є основною причиною порушень безпеки. Крім того, на хакерську діяльність впливають людські помилки. Освіта та обізнаність мають вирішальне значення для боротьби з кіберзлочинцями та запобігання порушенням безпеки.

Розглянуті поняття трактуються наступним чином: «Інформаційна безпека — це стан системи, здатний протистояти дестабілізуючій дії зовнішніх і внутрішніх інформаційних загроз з одного боку, і її функціонування — з іншого. не створює інформаційних загроз для елементів системи та зовнішнього середовища» [20].

Інформаційна безпека визначається як «захист інформації та інфраструктури, що її підтримує, за допомогою комплексу програмних, апаратних і програмних засобів і методів, а також організаційних заходів, з метою запобігання їх пошкодженню».

Подібне розкриття змісту розглянутого поняття спостерігається в і в інших джерелах [16]: «Інформаційна безпека — це захист інформації та підтримуючої інфраструктури від випадкових або навмисних впливів». Основна відмінність полягає в тому, що безпека розуміється як стан навколишнього середовища, а не як процес придбання, збереження та контролю.

Інформаційна безпека – це умова, яка дозволяє стабільно розвиватися та зберігати цілісність суб’єкта господарювання.

Кібербезпека та інформаційна безпека настільки тісно пов’язані, що їх часто вважають синонімами. Але між ними є кілька важливих відмінностей.
Кібербезпека стосується внутрішніх або сторонніх атак організації Це в основному основа для захисту всього, що піддається злому, атаці або несанкціонованому доступу, що складається з комп’ютерів, пристроїв, мереж, серверів і програм.

Таблиця 1.1

Відмінності кібербезпеки та інформаційної безпеки

Кібербезпека	Інформаційна безпека
Представляє собою практику захисту даних в інтернеті	Представляє собою захист інформації від неавторизованого користувача, доступу та змін або видалення даних для забезпечення конфіденційності
Призначена для захисту кіберпростору від кібератак	Займається захистом даних від будь-яких форм загроз
Призначена для захисту всього периметру в кіберсфері	Призначена для захисту інформації незалежно від сфери
Усуває небезпеку для кіберпростору	Займається захистом даних від усіх форм загроз
Попереджає кіберзлочини, кібермахінації	Бореться проти несанкціонованого доступу, порушень цілісності та розкриття інформації
Займається проблемами загроз, що виникають в кіберпросторі	Пов’язана з інформаційними активами та цілісністю, конфіденційністю

Кібербезпека також стосується лише захисту даних у цифровій формі - основна відмінність інформаційної безпеки полягає в тому, що вона стосується цифрових файлів. Отже, коли ми говоримо про кібербезпеку, ми автоматично говоримо про цифрові дані, системи та мережі.

Кібербезпека – це область інформаційних технологій, яка зосереджена на захисті систем, які включають електронні записи, пристрої відстеження даних, апаратне та програмне забезпечення, що використовується для надання послуг і керування ними. Кібербезпека зосереджена на запобіганні атакам шляхом захисту систем від несанкціонованого доступу, використання та розкриття даних. Основною метою є забезпечення доступності, конфіденційності та цілісності конфіденційних даних, які, якщо їх зламано, можуть поставити під загрозу життя.

Кібератаки можуть приймати різні форми, від програм-вимагачів до крадіжки особистих даних. Ефект атаки може змінюватися в залежності від розміру об'єкта. Кілька проблем є спільними для всіх галузей: захист конфіденційних особистих даних, уразливості в застарілих системах, проблеми IT і порушення безпеки. Інформаційна безпека (або «InfoSec») — це інший

спосіб сказати «інформаційна безпека» стосовно конфіденційності, цілісності та доступності.

Більшість сьогоднішньої бізнес-інформації зберігається в електронному вигляді на серверах, настільних комп’ютерах, ноутбуках або в Інтернеті, але десять років тому, до того, як усі конфіденційні дані були перенесені в Інтернет, вони зберігалися в картотеках.

Інформаційна безпека стосується безпеки даних у різних формах і є дещо ширшим поняттям, ніж кібербезпека.

Кібербезпека – це захист даних в електронній формі (таких як комп’ютери, сервери, мережі, мобільні пристрої тощо) від компрометації чи атак [18].

Частиною цього є визначення критично важливих даних, їх місцезнаходження, ризику та технології, яку необхідно застосувати для їх захисту. Кібербезпека та безпека даних також мають компонент фізичної безпеки.

Склад, наповнений конфіденційними паперовими документами, потребує фізичного захисту. Оцифрування даних вимагає використання передових засобів захисту даних. Оскільки неможливо поставити фізичний замок на стаціонарний комп'ютер, його можна повісити на двері серверної. Іншими словами, якщо дані зберігаються фізично або в цифровому вигляді, вам потрібно переконатися, що вони мають усі необхідні засоби контролю фізичного доступу, щоб запобігти несанкціонованому доступу.

Головним обов’язком бізнесу щодо інформаційної безпеки є захист даних комерційних компаній від будь-якого несанкціонованого доступу. Основним завданням бізнесу з кібербезпеки є захист даних компанії від несанкціонованого електронного доступу. Але в обох випадках цінність даних має першорядне значення [33].

Протягом останнього десятиліття ми спостерігали конвергенцію кібербезпеки та інформаційної безпеки, оскільки ці дві різні позиції злилися. Проблема полягає в тому, що в більшості команд немає спеціаліста з

інформаційної безпеки, тому обов’язки фахівця з кібербезпеки надзвичайно великі.

Просунуті фахівці з кібербезпеки традиційно розуміють, які технології, брандмауери та системи запобігання вторгненням потрібні, але вони не обов’язково пов’язані з бізнесом оцінки даних.

Кібербезпека - це особливий вид інформаційної безпеки. Способи, якими організації захищають цифрову інформацію, таку як мережі, програми, пристрої, сервери та інші цифрові активи.

Хоча це лише один з аспектів інформаційної безпеки (разом із фізичною безпекою), йому приділяється найбільша увага, оскільки кіберзагрози набагато сильніші, ніж фізичні.

Зловмисне програмне забезпечення, злочинні хакерські атаки та внутрішні помилки є основними причинами витоку даних, тому доцільно надавати пріоритет захисту, який зменшує ці ризики.

Незалежно від того, чи йдеться про кібербезпеку, чи про інформаційну безпеку в цілому, необхідно враховувати три стовпи інформаційної безпеки. Модель описує методи захисту конфіденційної інформації та включає:

1. Люди. Співробітники щодня мають справу з конфіденційною інформацією, тому організації повинні навчати їх про ризики та способи забезпечення безпеки.
2. Процеси: організації повинні документувати кроки, які вони вживають для забезпечення безпеки працівників. Це має включати визначення ролей і відповідальності за діяльність із захисту даних.
3. Технологія. Існує багато технічних засобів захисту, які організації можуть використовувати для боротьби із загрозами, наприклад, антивірусне програмне забезпечення, контроль доступу та шифрування даних.

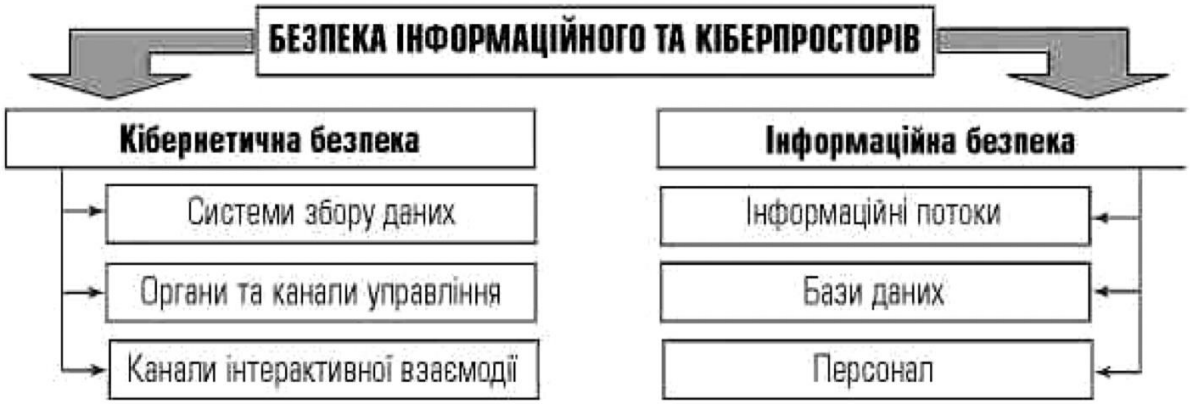

Рис.1. Обєкти впливу в інформаційному та кіберпросторі

Незважаючи на те, що в Інтернеті точаться гострі дискусії щодо того, чи означають кібербезпека та інформаційна безпека те саме, має сенс розглядати кібербезпеку як форму інформаційної безпеки. Інформаційну безпеку слід розглядати як парасольку, під яку потрапляють кібербезпека та інші теми безпеки, такі як криптографія та мобільні комп'ютери. Однак, враховуючи їхню відносну позицію в описовій ієрархії та вплив, чітке розмежування може бути непростим.

Кібербезпека та інформаційна безпека є критично важливими аспектами технологічного процвітання в 21 столітті.

РОЗДІЛ 2. АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ КРАЇН В УМОВАХ МІЖНАРОДНИХ КОНФЛІКТІВ

2.1. Аналіз кібербезпеки провідних країн світу

Кіберпростір став невід'ємною частиною життя кожної сучасної людини. Він сприяє вирішенню соціальних проблем і має великий потенціал з точки зору економічного зростання та інновацій, а світова спільнота розглядає його як стимул розвитку, який надає можливості для спілкування та соціальної взаємодії. Зважаючи на це, кібератаки на інформаційну інфраструктуру стали реальною загрозою та є одним із пріоритетних викликів національної безпеки та управління ризиками. У кіберпросторі розвиваються нові деструктивні практики, включаючи злочинне використання Інтернету (кіберзлочинність), шпигунство в політичних чи економічних цілях, атаки на критичну інфраструктуру (транспорт, енергетику, зв’язок тощо) з метою диверсій. Ці кібератаки, засновані на урядових або неурядових суб’єктах:

• не обмежені кордонами чи відстанями;

• є анонімними, і їх дуже важко ідентифікувати справжнього злочинця, часто діючи за допомогою ботнетів або посередників (проксі).);

• можна впровадити відносно легко з невеликими витратами чи ризиком для зловмисника.

Вони мають на меті порушити безперебійну роботу інформаційно-комунікаційних систем (ICS), якими користуються громадяни, підприємства та адміністрації, і навіть фізичну цілісність інфраструктури, критичної для національної безпеки.

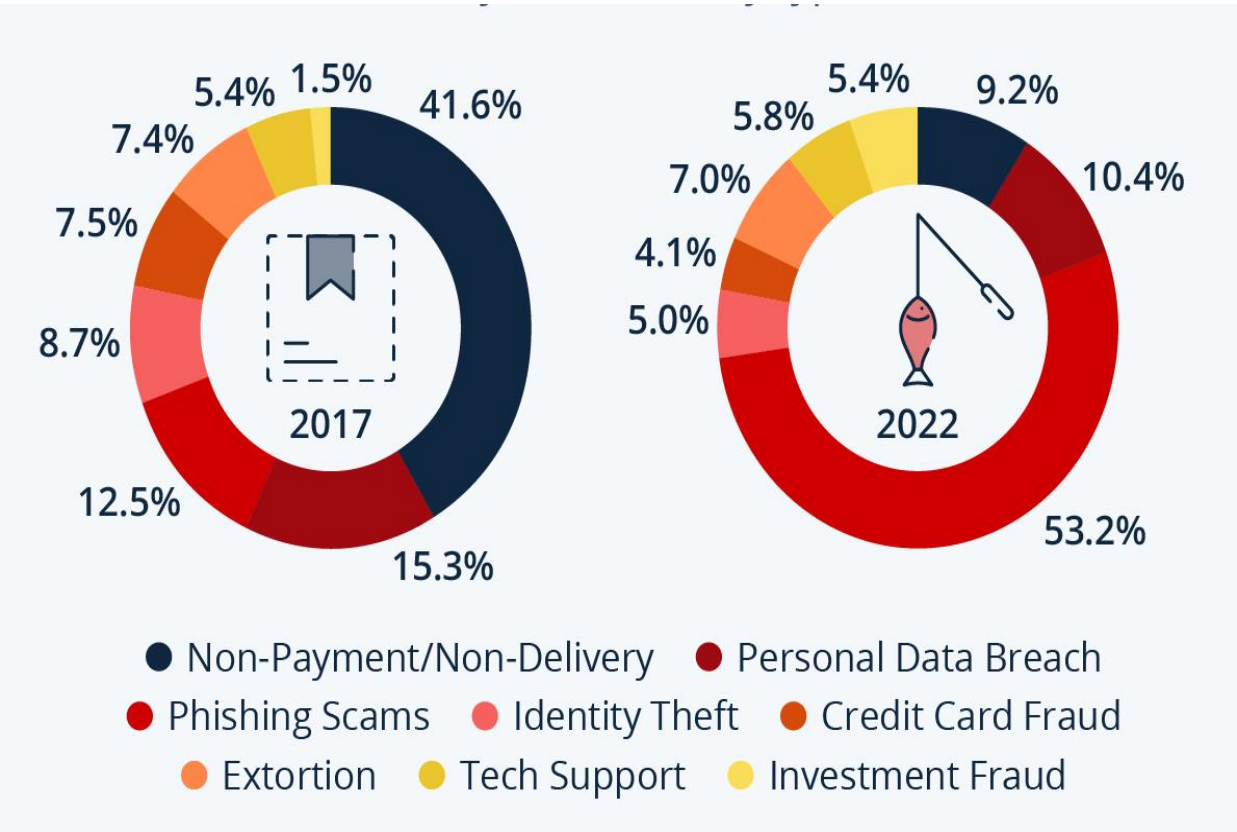

Рис. 2.1. Найбільш переважаючі форми кіберзлочинів

Джерело: побудовано автором на основі [22]

Кібербезпека включає всі заходи безпеки, які можна вжити для захисту від цих атак. Значне зростання складності та інтенсивності кібератак за останні роки змусило багато розвинених країн зміцнити свій захист і прийняти національні стратегії кібербезпеки. Тому актуальним у світі є питання забезпечення захисту кіберпростору.

Country	National Cyber Security Index (NCSI)	Global Cybersecurity Index (GCI) 2020	Cybersecurity Exposure Index (CEI) 2020*	Cyber-Safety Score (Mean Average of NCSI and GCI)
1. Belgium	94.81	96.25	81.00	**90.69**
2. Finland	85.71	95.78	89.00	**90.16**
3. Spain	88.31	98.52	79.00	**88.61**
4. Denmark	84.42	92.60	88.30	**88.44**
5. Germany	90.91	97.41	75.90	**88.07**
6. Lithuania	93.51	97.93	70.30	**87.25**
7. France	84.42	97.60	77.20	**86.41**
8. Sweden	84.42	94.55	79.00	**85.99**
9. UK	77.92	99.54	79.30	**85.59**
10. Portugal	89.61	97.32	69.70	**85.54**

Рис. 2.2. Топ-10 країн з найнижчим рівнем кіберзагроз

Джерело: побудовано автором на основі [28]

Стратегічні позиції, прийняті на найвищому політичному рівні в останні роки, зміцнили позицію кібербезпеки як пріоритету уряду. У 2008 та 2013 роках Франція провела глибокий перегляд своєї політики в галузі оборони та національної безпеки, а нові пріоритети були визначені та затверджені тодішнім президентом Французької Республіки. Серед них – запобігання кібератакам і реагування на них, які визначені як головні пріоритети національної безпеки [27].

У липні 2009 року, дотримуючись рекомендацій Білої книги з питань оборони та національної безпеки, було створено Французьке агентство мережевої та інформаційної безпеки (ANSSI, Національне агентство інформаційної безпеки) для вирішення зростаючої проблеми кібератак. ANSSI, міжміністерське агентство при офісі прем'єр-міністра, набуло популярності на початку 2011 року, коли агентство стало Національним органом безпеки інформаційних систем. Після створення агентства у 2011 році Франція опублікувала національну стратегію захисту та безпеки інформаційних систем. Біла книга 2013 року підтвердила кіберзагрозу та конкретно визначила ризик саботажу проти критичної інфраструктури. Стратегія кібербезпеки в Європейському Союзі була запропонована в лютому 2013 року Європейською Комісією та Європейською службою зовнішніх дій (EEAS). Франція активно сприяє реалізації п'яти основних напрямків [26]:

• Загальна стабільність ЄС (включаючи інституції ЄС);
• боротьба з кіберзлочинністю;
• Питання кіберзахисту в рамках загальної політики безпеки та оборони;
• промислові питання;
• міжнародна політика в кіберпросторі.

У країнах НАТО кіберзахист є ключовим аспектом оновлення альянсу та його адаптації до нових загроз. Після ухвалення нової стратегічної концепції на саміті в Лісабоні в листопаді 2010 року, політика НАТО щодо кіберзахисту була затверджена 28 червня 2011 року та «посилена» на саміті в Ньюпорті (Уельс) у вересні 2014 року. З появою Інтернету та концепції IoT (Інтернет речей) атаки

стають дедалі витонченішими, і їм важче запобігати та протидіяти [29]. Водночас Франція приділяє багато уваги, зусиль і ресурсів для вивчення світового досвіду та застосування його у власній країні, створюючи таким чином одну з найуспішніших систем боротьби з кіберзлочинністю. Важливо зазначити, що така серйозна система та важливі заходи безпеки не обмежують фундаментальних прав громадян, організацій та ЗМІ. Хоча наразі не існує ідеальної системи захисту від усіх можливих кіберзагроз, Франція впевнено будує свій кіберзахист, який дозволить їй проводити внутрішню та зовнішню політику без надмірних загроз і зберігати лідируючі позиції у вирішенні глобальних викликів.

Японія зарекомендувала себе як одна з найрозвиненіших інформаційних держав у світі і повинна забезпечити гідний рівень кібербезпеки, щоб зберегти свою репутацію. Діапазон груп, які постраждали від кібератак (від окремих осіб і приватних сімей до складних підприємств соціальної інфраструктури), стрімко розширюється. Незважаючи на всі зусилля японського уряду, загроза атак на дані продовжує зростати. Цей ризик впливає на такі сфери, як національна безпека, управління ризиками та конкурентоспроможність японської економіки. Японська промисловість відстала від своїх американських і європейських колег в оцінці кіберзагроз. Згідно з урядовою статистикою, лише 55 відсотків японських компаній проводять оцінку ризиків кібербезпеки, у порівнянні з приблизно 80 відсотками в США та 65 відсотками в Європі [25]. 10 червня 2013 року Рада з політики інформаційної безпеки Японії прийняла Стратегію кібербезпеки. Уряд Японії раніше використовував фразу «інформаційна безпека» для своєї політики та основних планів. Однак через зростання кіберзагроз, які виходять за рамки інформаційної безпеки, таких як саботаж об’єктів життєзабезпечення.

Для вирішення всіх цих проблем було вирішено вперше використати термін «кібербезпека». Стратегія спрямована на розвиток «провідного у світі», «стійкого» та «динамічного» кіберпростору та перетворення Японії на світове лідерство у сфері кібербезпеки. Для реалізації цих цілей документ передбачає

чотири основні принципи: забезпечення вільного обміну інформацією; вжиття нових заходів у відповідь на посилення ризиків; вжиття адекватних заходів проти кіберзагроз на основі оцінки ризиків; вжиття заходів та взаємодія з іншими країнами на основі їх соціальної відповідальності. Державним органом, що регулює відносини у сфері кібербезпеки, є Національний центр інформаційної безпеки (НЦІБ), який розробляє проекти державних стандартів заходів інформаційної безпеки, розробляє рекомендації за результатами оцінки стану кібербезпеки та сприяє стану кібербезпеки. реалізація заходів щодо покращення стану кібербезпеки [19].

До прикладу, Китай вразливий, оскільки йому не вистачає єдиної стратегії. Основні завдання, які Китай поставив перед собою у сфері кіберзахисту:

1. Захист суверенітету кіберпростору
2. Захист критичної інформаційної інфраструктури (CI)
3. Створення пильної онлайн-культури
4. Боротьба з кіберзлочинністю, шпигунством і тероризмом
5. Удосконалення кіберуправління
6. Покращення базової кібербезпеки
7. Посилення міжнародного співробітництва [23]

У наступні рік-два Китай продовжуватиме контролювати інформацію та технології за допомогою CSL та відповідних нормативних актів. Локалізація даних, особливо для «критичних» даних, необхідна для всіх компаній, які працюють у Китаї. Регулятори також зобов’язуються «безпечно та контрольовано» (наприклад, шифрування) використовувати технології, які відповідають їхнім вимогам.

Зусилля з правозастосування й надалі будуть зосереджені насамперед на системах та інформації урядових установ Китаю, а також державних і приватних підприємств, які дуже серйозно сприймають такі кіберзагрози, про що свідчать нормативні документи, що регулюють прийняту політику кібербезпеки та основні заходи протидії. ворожих груп. Південна Корея. Частота та серйозність кібератак спонукали уряд Південної Кореї переглянути свою стратегію

кібербезпеки. Існує три агентства, які займаються питаннями кібербезпеки: Національний центр кібербезпеки, Корейське агентство Інтернету та безпеки (KISA) і Центр кібертероризму Національного агентства поліції. Ці агентства відповідають за виявлення, запобігання та реагування на кібератаки та загрози безпеці. Крім того, була створена школа, що спеціалізується на кібервійні, з наміром збільшити кількість експертів з безпеки до 7000 до кінця 2019 року [27].

Майбутнє системи захисту кіберпростору Південної Кореї:

− шифрування для доступу до мережі;

- Системи запобігання вторгненням (IPS);

- розширена постійна загроза (APT);

- хмарні обчислення;

− Безпека Інтернету речей

У американських фірм є багато можливостей надавати найсучасніші рішення з кібербезпеки для критичної інфраструктури в Південній Кореї. Завдяки розвиненій інфраструктурі ІКТ Південна Корея є ідеальним ринком для американських фірм, які хочуть перевірити свої рішення з кібербезпеки, перш ніж виходити на інші ринки. Щоб вийти на ринок кібербезпеки [29].

Комерційна служба США в Кореї рекомендує американським технологічним компаніям співпрацювати з провідними південнокорейськими компаніями, які підтримують існуючі торговельні мережі на фінансових, енергетичних та інших ключових інфраструктурних ринках і мають глибоке розуміння особливостей місцевого ринку та унікальні нормативні вимоги. .UK.Загальновідомо, що Велика Британія - країна, яка дуже ретельно зберігає свої секрети. Прикладом цього може бути, зокрема, історія систем шифрування з відкритим ключем. Його алгоритм був вперше розроблений і опублікований у 1977 році вченими Массачусетського технологічного інституту Рональдом Райвестом, Аді Шаміром і Леонардом Адлеманом. Хоча лідерство в цьому питанні належить британським вченим Кліффорду Коксу і Малкольму Вільямсону, які зробили це в 1973 році, сам алгоритм і його використання були засекречені до 1997 року [15]. Сучасна система кіберзахисту потребує

високоталановитого персоналу, який відповідна спецслужба шукає серед різних груп населення. NCSC розробив серйозну систему підбору персоналу. Для цього кожен в організації, який вивчає прикладні технології, математику чи мову, отримує можливість брати участь у реальних проектах. Програма CyberFirst є ключовою частиною Національної програми уряду. Він пропонує широкий спектр заходів, стипендіальних програм, літніх шкіл тощо. це включає. Це програма для студентів і талановитої молоді, яку проводить NCSC, яка пропонує комплексний пакет фінансової допомоги та навчання кібернавички для талановитих початківців. Ретельний аналіз закритих і діючих програм показує, що цільова аудиторія з кожним роком молодшає. Найбільш вражаюче те, що деякі з пропозицій тепер стосуються молодих людей, які закінчили навчання між 2020 і 2023 роками. Проте з відмінними оцінками з предметів STEM. Зокрема, люди з особливими потребами можуть претендувати на роботу в системі GCHQ, але вимоги щодо найближчого оточення, громадянства Великобританії та проживання в країні протягом останніх 10 років безсумнівні. . Опубліковано 29 листопада 2018 р. Як і з іншими матеріалами, інтересам національної безпеки Великобританії найкраще служить зберігання та накопичення знань, а не їх виробництво. Існує два способи боротьби з кіберуразливістю. По-перше, це виявити вразливість, щоб її можна було виправити та принести користь глобальним користувачам технологій.зберегти знання про цю вразливість і використовувати їх для майбутніх розвідувальних цілей і перешкоджати діяльності тих, хто шукає шкоди у Великобританії [16]. Рішення на користь одного з цих методів приймається групою провідних світових експертів з трьох агентств (GCHQ, NCSC і Міністерства оборони).

На саміті з кібербезпеки Біллінгтона у Вашингтоні, округ Колумбія, 13 вересня 2016 року керівник NCSC Кіаран Мартін підкреслив, що «…хоча сьогоднішня робота в галузі кіберзахисту вимагає відкритого підходу, вона вимагає дуже відкритого підходу» важливо зберегти статус Великобританії як однієї з небагатьох суверенних криптографічних націй щодо її найважливіших («найчутливіших») таємниць» [27]. Високим рівнем роботи Британського

національного центру кібербезпеки є саме цей відділ, який у першому кварталі 2018 року був визнаний Microsoft у рамках програми Microsoft Bug Bounty, 5 найефективніших, отримав визнання заслуг і винагорода 15 000 доларів [28]. Як самодостатня суверенна нація, Сполучене Королівство має свої власні стандарти, від дорожніх знаків у милях і ярдах до молочних пляшок у пінтах, до спеціального дизайну розеток і до серйозних питань засобів до існування. Водночас ця країна не менш прагне до різних видів співпраці. Навпаки, це викликає велику повагу та інтерес

2.2 Аналіз впливу кібератак на кібербезпеку України в умовах військового конфлікту

24 лютого 2022 року російська федерація здійснила чергове військове вторгнення в Україну, порушивши Статут ООН. Триваючий міжнародний збройний конфлікт викликає занепокоєння щодо шкоди та наслідків, заподіяних цивільному населенню, а також щодо захисту цивільних осіб та цивільної інфраструктури, на які впливають як кінетичні, так і кібератаки.

Термін кібервійна, який використовується для позначення методу ведення війни, за допомогою якого державні та недержавні суб’єкти прагнуть проникнути в інший комп’ютер або мережу, щоб завдати шкоди чи збою, регулярно використовується в цій загарбницькій війні. Хоча експерти розходяться в думці щодо точного масштабу, впливу та важливості російських кібератак і операцій для досягнення стратегічних цілей країни, кіберпростір зараз є усталеною сферою конфлікту, яка швидко розвивається.

Як нова європейська оборонна доктрина, схвалена Європейською радою в березні 2022 року, Стратегічний компас визнає кіберсферу ведення війни, яку необхідно захищати шляхом співпраці та тісної координації. Це важлива зміна парадигми політики ЄС, яка традиційно наголошувала на кіберстійкості з позиції економічного впливу, а не оборони.

Багатовимірна війна, яка використовується в триваючому збройному конфлікті в Україні, становить складний виклик безпеці.

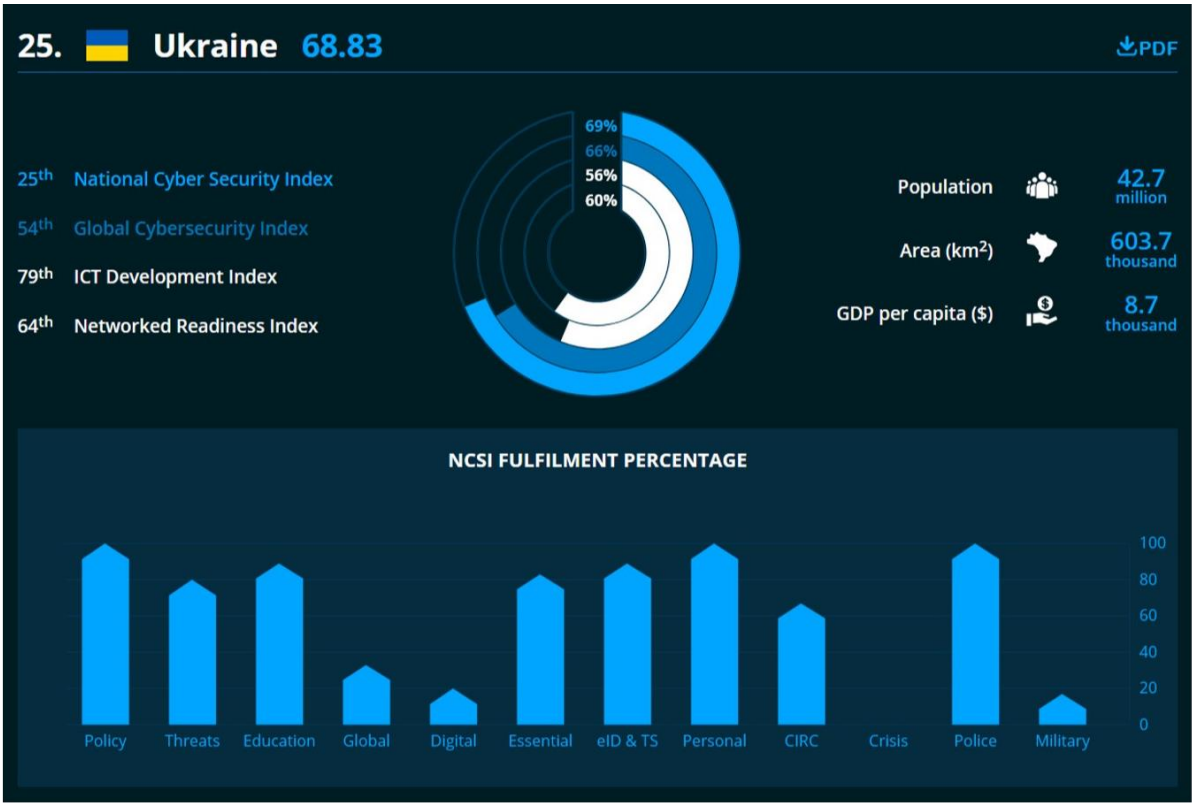

Рис. 2.3. Національний індекс кібербезпеки України (2023 р.)
Джерело: побудовано автором на основі [29]

Застосування кібератак і операцій у мирний час і під час збройних конфліктів сьогодні є реальністю. Територіальне вторгнення збройних сил російської федерації в Україну в лютому 2022 року супроводжувалося руйнівними кібератаками, і яскраво демонструє цю тенденцію. Використання кібератак як засобу ведення війни також спостерігалося раніше між державами, включаючи російську федерацію та Грузію, Ізраїль та Іран, російську федерацію та Україну (зокрема, росія розгортає кібератаки проти України з 2014 року) [30]. Інститут CyberPeace документує кібератаки на критичну інфраструктуру та цивільні об’єкти з початку російсько-агресорської війни проти України. Документування атак сприяє аналізу використання кіберзасобів у воєнний час.

Станом на 31 травня 2023 року Інститут зафіксував 1998 кібератак і операцій, здійснених 98 різними суб'єктами. Ці кіберінциденти були спрямовані на 23 різні сектори критичної інфраструктури, вплинувши на Україну, російську федерацію та близько 49 інших країн [29].

Ця сукупність даних показує, що обсяг і розмах кібератак проти України були дуже високими і привернули б набагато більше уваги за інших обставин (якби не було кінетичних атак). Спостережувані атаки не є інноваційними щодо використовуваних технологій чи методів, але кількість атак, виконавці та використання кібернетичних засобів проти критичної інфраструктури викликають тривогу. Крім того, спостерігаються зв'язки між різними типами атак. Кібератаки та операції зараз є усталеним типом військових операцій, які координуються або синхронізуються навколо кінетичних військових операцій. Саме ця комбінація кінетичних і кібератак має такий глибокий вплив на цивільне населення, впливаючи на критичну інфраструктуру та цивільні об’єкти, від яких вони залежать, включно з інформаційним простором. Це поєднання є руйнівним і дестабілізуючим.

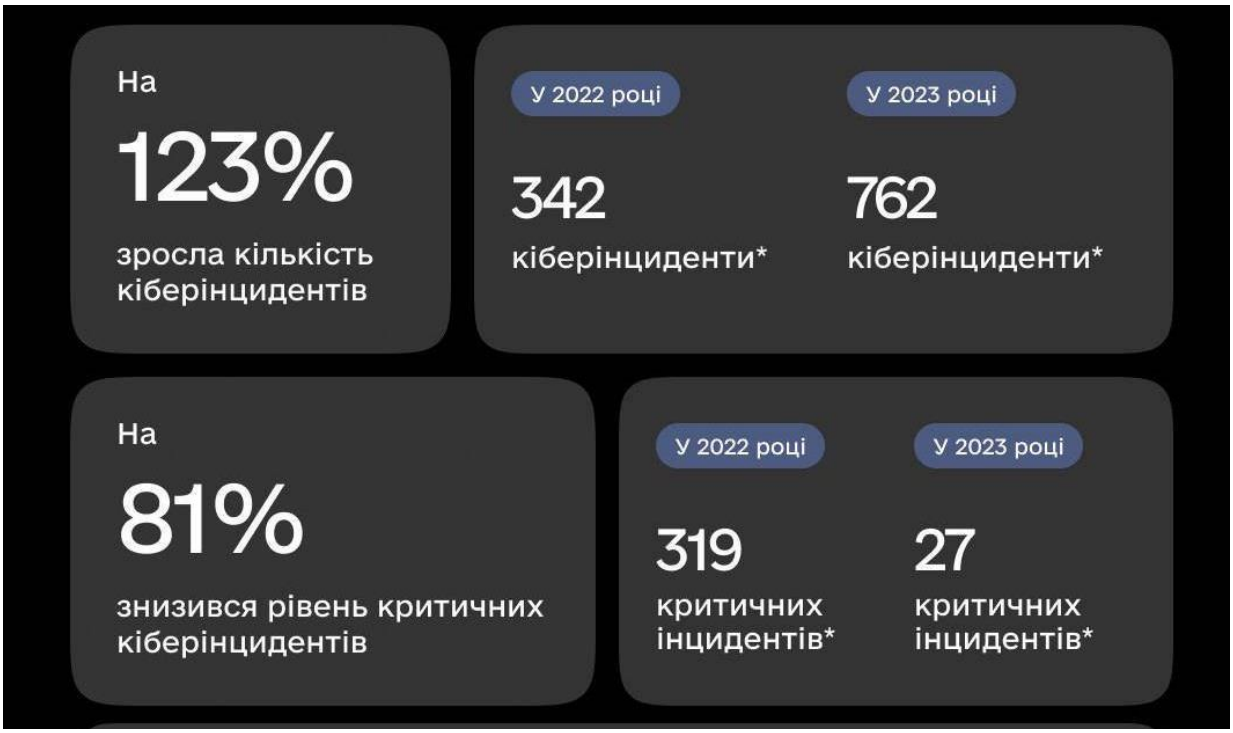

Рис. 2.4. Кібервійна з росією: головні цифри за січень-червень 2023 року

Джерело: побудовано автором на основі [31]

У контексті військових дій, таких як війна в Україні, саме використання звичайних озброєнь наразі має більш видимий і більш вимірний вплив. Проте, як підкреслив Крістіан-Марк Ліфландер, керівник Відділу нових викликів безпеці (ESC) Секції кібер- та гібридної політики (CHP) НАТО: «На відміну від нарощування військ або інших форм військової мобілізації, які є нечастими та дуже помітними, кібероперації є результатом оперативних циклів, які відбуваються приховано та постійно протягом мирного та воєнного часу [26]. Націлювання на чутливі мережі в мирний час дозволяє зловмисникам закласти основу для зловмисного програмного забезпечення, призначеного для використання під час війни. Методи, які зловмисники використовують для встановлення початкових точок шпигунської діяльності, не відрізняються від тих, які передують кібератакам. Для кіберпідрозділів війна принципово не змінює спосіб підготовки або початку бою.

Зведені дані, зібрані та проаналізовані Інститутом кібермиру, підтверджують зауваження про те, що важливо вийти за межі упереджених уявлень про роль, яку відіграватимуть кібератаки під час війни, і про роль, яку вони відіграють у військових операціях росії [27].

Спостереження за використанням кібернетики в інших контекстах підтверджують це. Під час конфлікту з метою знищення та шифрування даних і систем активно використовувалися програми очищення шкідливих програм. Наприклад, атака на супутникову мережу Viasat призвела до відключення доступу до Інтернету більше ніж на два тижні [19].

У Франції 9 000 абонентів супутникового інтернет-провайдера позбавили інтернету. Близько третини з 40 000 абонентів іншого супутникового інтернет-провайдера в Європі постраждали, а велика німецька енергетична компанія втратила доступ до дистанційного моніторингу понад 5 800 вітрових турбін. Атака зловмисного програмного забезпечення 25 лютого 2022 року на пункт прикордонного контролю сповільнила процес пропуску біженців до Румунії [23].

Кібератаки з підривними елементами призвели до блокування доступу до телекомунікаційних та інтернет-послуг, обмеження доступу до грошей, переривання доступу до новин, а в минулому, як було показано, призводили до відмови в доступі до електроенергії, опалення та води.

Наприклад, 28 березня 2022 року атака на «Укртелеком» призвела до обвалу зв'язку на 13% від довоєнного рівня, причому спостерігався збій у всій країні. Поширення дезінформації та пропаганди, в тому числі через атаки на медіа-сектор, дестабілізують, оскільки впливають на інформаційний простір та обмежують доступ населення до своєчасної, достовірної та офіційної інформації. Це підриває довіру до інституцій шляхом маніпулювання інформацією [20]. Компрометація даних – зламаних і витоку даних, зокрема колективами хакерів – призводить до публікації величезних обсягів даних про організації та окремих осіб в Інтернеті з невідомими довгостроковими наслідками.

Нарешті, важливо підкреслити важливість ефективності кіберзахисту України для відбиття атак та/або пом'якшення їхнього впливу.8. Україна підвищила стійкість своєї національної інфраструктури інформаційно-комунікаційних технологій (ІКТ) і реагування на кіберінциденти до та під час війни у співпраці з урядами країн-членів і приватними компаніями.

Приватний сектор України також зробив великий внесок у цей процес. Це включало діяльність із посилення кіберстійкості України до та після військових вторгнень у 2014 і 2022 роках, а також співпрацю з Центром передового досвіду спільного кіберзахисту НАТО (CCDCOE) [30].

Підготовка України, визнаючи, що вона була об'єктом кібератак протягом багатьох років, включала приватно-державне партнерство. З початком війни приватні гравці, такі як Microsoft, Google, Amazon і ESET, публічно визнали свою роль у відстеженні та прогнозуванні кіберзагроз, розміщення державних даних у публічній хмарі за межами України та інші форми співпраці з Урядом України для запобігання кіберзагрозам.

РОЗДІЛ 3. СТРАТЕГІЯ ЗАПОБІГАННЯ НАСЛІДКАМ КІБЕРАТАК

Кіберпростір став місцем конфлікту між державами, а також нетрадиційними гравцями. Вважається новим полем бою, таким як повітря, земля, море та космос. Це визнає НАТО, яка визнала кіберпростір зоною військових операцій у 2016 році. Держави-члени також повинні покращити розуміння процедур реалізації та сценаріїв вправ для взаємної допомоги та/або солідарності відповідно до статті 42 [18]. Стаття 222 Договору про Європейський Союз (ДЄС) та Договору про функціонування Європейського Союзу (ДФЄС). Стратегічний компас EU47 визнає кіберсферу війни. Крім того, все більше і більше країн розвивають військові кіберпотенціали, що збільшить їх використання в наступальних і оборонних операціях [26].

Хоча повний масштаб і наслідки кібератак і операцій, пов’язаних з агресивною війною росії проти України, ще оцінюються та визначаються, перші уроки вказують на важливість посилення захисту цивільної інфраструктури, яка надає критичні послуги населенню. Триваюча війна проти України пропонує важливі спостереження та міркування щодо покращення розуміння ЄС кібервимірів кіберстійкості держав-членів, таких як масштаби збитків і втрат, отримані уроки та важливість залучення багатьох зацікавлених сторін. спроба.

Важливі висновки, пов’язані з триваючою війною в Україні, включають збільшення кількості кібератак і операцій із залученням громад, підпорядкованих воюючим країнам. Це призводить до цивілізації та краудсорсингу війни, юридичних міркувань, важливих для війни, а також прямої та непрямої участі у бойових діях. Деескалацію кібервиміру конфлікту буде складно, навіть якщо буде досягнуто згоди щодо припинення бойових дій та/або припинення вогню, оскільки кібервиміри такого припинення або припинення вогню буде дуже важко контролювати [29]. Крім того, кібервимір ускладнюється зв’язком між кінетичною війною, кібератаками та розповсюдженням шкідливого контенту49. Крім того, можна спостерігати негативні наслідки кібератак для невоюючих країн, крім двох воюючих країн. Повний масштаб таких атак важко

оцінити без самоопису суб'єкта загрози, ідентифікації прихильності до однієї з двох воюючих країн і доказів наміру цих атак. Що ще важливіше, кібератаки та операції були націлені на широкий спектр організацій. Важливо розуміти, які організації, мережі та системи зазнали негативного впливу, щоб зосередити зусилля з відновлення там, де вони найбільше потрібні, наприклад, відновлення після атак зловмисного програмного забезпечення. Деякі атаки мають наслідки, які стають очевидними з часом і потребують років, щоб відновитися, наприклад потенційні наслідки витоку даних і крадіжки з боку організації ядерної безпеки.

Агресійна війна росії проти України підкреслила необхідність посилення можливостей кіберзахисту шляхом спільної співпраці між державами-членами. Це включає зменшення стратегічної залежності ЄС від критичних кібертехнологій та зміцнення європейської оборонної технологічної та промислової інфраструктури (EDTIB) [23]. Загрози кібербезпеці зросли в масштабах, частоті та складності. Перехід до безнадійного підходу до критичних кібертехнологій може підтримати колективну оборону ЄС шляхом зменшення потенційної вразливості та впливу загроз, що розвиваються. Підхід Zero Trust також відповідає принципам GDPR, обмежує доступ до конфіденційних даних і забезпечує високі стандарти авторизації користувачів.

Краще розуміння загроз кібербезпеці ЄС, які виникають через поточне та потенційне використання кіберактивів у збройних конфліктах і в мирний час, потребує підходу, орієнтованого на людей, заснованого на законі та правах людини. Важливо визнати важливість і масштаби цивільної шкоди та наслідків від скоординованого використання кінетичних військових операцій і кібероперацій під час збройного конфлікту, а також впливу кібератак за межі кордонів воюючих країн. Кібератаки, інформаційні операції та кінетичні атаки тісно пов'язані між теперішньою та майбутньою війною. Цей зв'язок важливий для розуміння скоординованих атак в Україні, їх впливу на сектори критичної інфраструктури та операцій кібервпливу, спрямованих на різні аудиторії, включно з територіями за межами воюючих країн. Така координація створює потребу в новому підході, який виходить за рамки розгляду окремих типів атак і

спрямований на єдину кіберстійкість, готовність і захист. Держави-члени повинні мати можливість реагувати на загрози шляхом розуміння загроз на основі доказів, координації законодавчих зусиль ЄС і співпраці між науковими дослідженнями, урядами, приватним сектором, громадянським суспільством і академічними колами.

Забезпечення стійкості кіберзахисту є дуже важливим завданням для сучасної держави, особливо під час збройного конфлікту. Ефективний кіберзахист передбачає розробку комплексної стратегії, яка включає кілька аспектів, спрямованих на запобігання, виявлення та реагування на кібератаки:

1) Розвиток кіберінфраструктури. Системи захисту мережі та інформації включають антивіруси, брандмауери, системи виявлення вторгнень, шифрування даних та інші технології. Вони призначені для виявлення та усунення загроз у реальному часі. Постійне оновлення цих систем має вирішальне значення для підтримки кібербезпеки.

2) Охорона критичних об'єктів. Критичні об’єкти, такі як енергетичні системи, транспорт, банківські установи та комунікації, потребують особливого захисту. Вони можуть стати об’єктом спроб знищити або розкрити секретну інформацію. Необхідно посилити їх захист і використовувати резервні системи.

3) Навчання співробітників. Ефективний кіберзахист вимагає підготовки надійного персоналу. Безперервна освіта та тренінги з кібербезпеки можуть допомогти підвищити знання та обізнаність співробітників і урядовців. Навчання має включати розпізнавання загроз, процедури реагування та запобігання соціальної інженерії.

4) Залучення експертів. Доступ до експертів з кібербезпеки, внутрішніх і зовнішніх консультантів є критично важливим під час збройних конфліктів. Вони надають професійну експертизу щодо кіберзагроз і допомагають розслідувати інциденти.

5) Відновлення після кібератаки. Повинні бути розроблені плани подолання кібератак, включаючи процедури відновлення інфраструктури та даних,

охоплення спільноти та відновлення. Це допомагає скоротити час відновлення інциденту.

6) Співпраця з іншими країнами. Під час збройних конфліктів важливо співпрацювати з іншими державами в обміні інформацією про кіберзагрози та спільні заходи протидії. Міжнародне співробітництво є ключовим елементом стійкості кіберзахисту.

7) Співпраця з приватним сектором. Приватні компанії, які володіють критично важливою інфраструктурою, також повинні бути включені до своїх планів кіберстійкості. Робота з ними допомагає швидше й ефективніше виявляти загрози та реагувати на них.

8) Захист важливої інформації. Інформація має бути захищена від несанкціонованого доступу за допомогою шифрування, контролю доступу та резервного копіювання.

9) Планування на випадок надзвичайних ситуацій. Окрім відновлення після кібератаки, важливо мати плани на випадок надзвичайних ситуацій, такі як евакуація персоналу, зв’язок у разі відключення Інтернету чи електроенергії та інші заходи для забезпечення безпеки та стабільності.

10) Роль державних інституцій у забезпеченні кіберзахисту. Урядові інституції відіграють ключову роль у забезпеченні кіберзахисту, розробляючи та впроваджуючи політику та стратегії кібербезпеки. Вони відповідають за запобігання кібератакам, виявлення загроз та ефективне реагування на них.

11) Нормативно-правове регулювання кібербезпеки. Державні інституції створюють закони та політику, які регулюють кібербезпеку. Це включає прийняття законів, які криміналізують кіберзлочинність і встановлюють відповідальність за порушення кібербезпеки.

12) Розробка стандартів і нормативів. Держави розробляють стандарти для важливих для національної безпеки галузей, таких як енергетика, фінанси, транспорт і зв’язок. Ці стандарти визначають вимоги до кібербезпеки та регулюють заходи захисту критично важливих об’єктів.

13) Роль військових і правоохоронних структур. Військові структури відповідають за виявлення, перевірку та захист військових мереж і інформації, а також за розробку кіберстратегій і військової доктрини. Правоохоронні органи розслідують і переслідують кіберзлочини та виявляють загрози національній безпеці в кіберпросторі.

14) Співпраця з приватним сектором та науковими установами. Приватний сектор володіє більшістю критичної інфраструктури, тому співпраця з ним важлива. Урядові установи також співпрацюють з науковими установами для дослідження кібербезпеки та розробки нових технологій.

15) Фінансування та ресурси. Для ефективного кіберзахисту держави повинні виділяти достатньо коштів і надавати кваліфікований персонал для впровадження кібербезпеки.

16) Міжнародний аспект стійкості кіберзахисту. Співпраця між державами та дотримання міжнародних норм і правил у кіберпросторі сприяють стабільності та безпеці. Це включає укладання міжнародних угод, участь у спільних ініціативах та координацію дій у разі кібератак.

17) Міжнародне право та норми. Кібероперації повинні відповідати основним принципам міжнародного права, включаючи невтручання в суверенітет і імунітет держав, закріплені в Статуті ООН. Міжнародні кібернорми допомагають встановлювати правила в кіберпросторі.

18) Міжнародні спільні ініціативи. Держави укладають міжнародні угоди та беруть участь у форумах для обміну ідеями та досвідом щодо кібербезпеки. Спільні зусилля під час кібератак передбачають обмін інформацією та координацію дій.

Забезпечення стійкості кіберзахисту в умовах збройних конфліктів потребує комплексного підходу та співпраці на національному та міжнародному рівнях. Важливо розвивати кіберінфраструктуру, навчати співробітників і створювати кризові плани для відновлення після кібератак. Дотримання міжнародних норм і співпраця між державами забезпечує стабільність і безпеку в кіберпросторі.

ВИСНОВОК

Кібербезпека в умовах міжнародних конфліктів є критично важливою складовою національної безпеки кожної держави. Сучасні міжнародні конфлікти дедалі більше переносяться у кіберпростір, де загрози стають більш різноманітними та витонченими. Основні виклики, що постають перед країнами, включають атаки на критичну інфраструктуру, вразливість енергетичних, транспортних, комунікаційних систем, що потребує підвищеної уваги та посиленої захищеності. Дезінформаційні кампанії стають все більш потужним інструментом маніпуляції громадською думкою та дестабілізації соціально-політичної ситуації. Кібершпигунство та економічні загрози, такі як крадіжка інтелектуальної власності, комерційних та державних таємниць, ставлять під загрозу економічну стабільність та розвиток.

Для ефективної протидії кіберзагрозам необхідно розробити та впровадити комплексні стратегії, що включають міжнародне співробітництво, створення та підтримку альянсів і коаліцій для обміну інформацією та спільних дій у сфері кібербезпеки, технологічні інновації, впровадження передових технологій та інструментів для виявлення, запобігання та реагування на кіберзагрози, підвищення обізнаності та навчання, розробку програм для навчання фахівців та громадян з питань кібербезпеки, підвищення рівня кіберграмотності, а також законодавче регулювання, прийняття та вдосконалення нормативно-правової бази, що регламентує діяльність у кіберпросторі, забезпечує захист прав та свобод громадян. В умовах зростаючих кіберзагроз жодна держава не може залишатися осторонь. Спільні зусилля, координація дій та інноваційний підхід до кібербезпеки є ключовими елементами для забезпечення стабільності та безпеки в сучасному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Cybersecurity strategy (2018) URL: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

2. China publishes first national cybersecurity-strategy URL: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.

3. Cyberspace Administration of China URL: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

4. China's Cyber Security Law: how prepared are you? URL: https://www.controlrisks.com/campaigns/china-business/chinas-cyber-security-law.

5. Welcome to GCHQ.Pioneering a new kind of security for an ever more complex world URL:www.gchq.gov.uk.

6. Equities process Publication of the UK's process for how we handle vulnerabilities.URL: www.ncsc.gov.uk/blog-post/equities-process.

7. Tencent Xuanwu Lab Security URL: http://blogstechnet.microsoft.com/msrc/2018/04/20/recognizing-q3-top-5.

8. A new approach for cyber security in the UK(2016) URL: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk.

9.Кондакова С.В. Кібербезпека в Великобританії. Перші враження. –2019. – No 1.

10. K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

11. G. N. Reddy and G. J. U. Reddy, "a study of cyber security challenges and its emergning trends on latest technologies."

12. N. Shafqat and A. Masood, "Comparative Analysis of Various National Cyber Security Strategies," 2016. [Online]. URL: https://sites.google.com/site/ijcsis/

13. D. Craigen, N. Diakun-Thibault, and R. Purse, "Technology Innovation Management Review Defining Cybersecurity," 2014. [Online]. URL: www.timreview.ca

14. M. D. Richardson, P. A. Lemoine, W. E. Stephens, and R. E. Waller, “Educational Planning,” 2020.

15. D. Craigen, N. Diakun-Thibault, and R. Purse, “Technology Innovation Management Review Defining Cybersecurity,” 2014. [Online]. URL: www.timreview.ca.

16. D. Schatz, R. Bashroush, and J. Wall, “Towards a More Representative Definition of Cyber Security,” *The Journal of Digital Forensics, Security and Law*, 2017, doi: 10.15394/jdfsl.2017.1476.

17. S. P.S, N. S, and S. M, “Overview of Cyber Security,” *IJARCCE*, vol. 7, no. 11, pp. 125–128, Nov. 2018, doi: 10.17148/ijarcce.2018.71127.

“Cyber Security Applications Freeware & Shareware”.

18. P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, vol. 6, no. 2. Chongqing University of Posts and Telecommunications, pp. 147–156, May 01, 2020. doi: 10.1016/j.dcan.2019.01.005.

19. M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, “Cyber security in New Space: Analysis of threats, key enabling technologies and challenges,” *Int J Inf Secur*, vol. 20, no. 3, pp. 287–311, Jun. 2021, doi: 10.1007/s10207-020-00503-w.

20. Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, “Artificial intelligence and problems of ensuring cyber security,” *International Journal of Cyber Criminology*, vol. 13, no. 2, pp. 564–577, Jul. 2019, doi: 10.5281/zenodo.3709267.

21. P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, vol. 6, no. 2. Chongqing University of Posts and Telecommunications, pp. 147–156, May 01, 2020. doi: 10.1016/j.dcan.2019.01.005.

22. M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, “Cyber security in New Space: Analysis of threats, key enabling technologies and challenges,” *Int J Inf Secur*, vol. 20, no. 3, pp. 287–311, Jun. 2021, doi: 10.1007/s10207-020-00503-w.

23. D. Ghelani, Diptiben Ghelani., “Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review,” *American Journal of Science, Engineering and Technology*, vol. 3, no. 6, pp. 12–19, 2022, doi: 10.22541/au.166385207.73483369/v1.

24. Z. el Mrabet, N. Kaabouch, H. el Ghazi, and H. el Ghazi, “Cyber-security in smart grid: Survey and challenges,” *Computers and Electrical Engineering*, vol. 67, pp. 469–482, Apr. 2018, doi: 10.1016/j.compeleceng.2018.01.015.

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

26. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. – Київ : НІСД, 2022. – 456 с.

27. Даник Ю.Г. Основи кібербезпеки та кібероборони / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

28. Всеохоплююча оборона України: стан, проблеми та заходи щодо зміцнення кібероборони держави і створення кібервійськ. URL : https://opk.com.ua/

29. Кібератаки на Україну. URL : https://uworld.news/news/kiberataky-rosii-na-ukrainu-ie-1002005.html

30. Buchan, J., Carr, M., & Hancock, C. (2018). Cyber Resilience: A Review of Critical National Infrastructure in the UK. International Journal of Disaster Risk Reduction, 27, 145-152.