Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Кібервійна: сучасний стан, виклики та загрози
(назва теми)

Виконав: студент 6 курсу, групи БК-812м

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних мереж

КЛАДЬКО К.С
(ПРІЗВИЩЕ та ініціали)

Керівник РОМАНЕНКО С.М.
(ПРІЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О. Ю.
(ПРІЗВИЩЕ та ініціали)

2023

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри ІБтаН
Андрій КОРОТУН
«____» _____2023року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

КЛАДЬКА Кирила Сергійовича
(ПРІЗВИЩЕ, ім'я, по батькові)
1. Тема проєкту (роботи) Кібервійна: сучасний стан, виклики та загрози Cyber warfare: current state, challenges and threats

керівник проєкту (роботи) к.т.н., РОМАНЕНКО Сергій Миколайович,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 475
2. Строк подання студентом проєкту (роботи) 10 грудня 2023 року
3. Вихідні дані до проєкту (роботи) Проаналізувати поточний стан кібервійни. Ознайомитись з загрозами та наслідками. Проробити сценарій кібератаки на інфраструктурний об'єкт. Розробити ряд рекомендацій для підвищення рівню безпеки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд кібератак. Аналіз попередніх атак. Аналіз історії кібервійн. Рекомендації щодо захисту в кібервійні.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), 11 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 4	РОМАНЕНКО С. М., доцент. кафедри ІБтаН	04.09.2023	08.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент. кафедри ІБтаН		09.12.2023

7. Дата видачі завдання «04» вересня 2023року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження.	04.09.23 – 18.09.23	Виконано
2.	Відбір інформації та літератури, що відповідає отриманому завданню.	19.09.23 – 04.10.23	Виконано
3.	Аналіз кібервійн.	27.09.23 – 10.10.23	Виконано
4.	Вивчення тенденцій та історії кібервійн	11.10.23 – 15.10.23	Виконано
5.	Дослідження викликів та загроз кібервійн	16.10.23 – 24.10.23	Виконано
6.	Аналіз сучасного стану кібервійн	24.10.23 – 05.11.23	Виконано
7.	Моделювання сценаріїв кібератак	05.11.23 – 14.11.23	Виконано
8.	Розроблення рекомендацій	15.11.23 – 25.11.23	Виконано
9.	Оформлення матеріалів магістерської роботи.	25.11.23 – 05.12.23	Виконано

Студент _____ Кирило КЛАДЬКО
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Сергій РОМАНЕНКО
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи 78 с., 11 рис., 26 джерел.

КІБЕРВІЙНА, КІБЕРАТАКИ, КІБЕРЗАГРОЗИ, КІБЕРБЕЗПЕКА ФІШИНГ, ЗАХИСТ, ДЕФЕЙС, DDOS, OSI, NATO, OON, ES, PRIVACY, DATA, BREACHES, MALWARE, CYBERCRIME, CRITICAL, INFRASTRUCTURE.

Об’єкт дослідження – кібервійни, та кібервійна в контексті України.

Предмет дослідження – аналіз кібервійни та розробка рекомендацій для боротьби з кіберзагрозами.

Мета роботи – аналіз сучасного стану, викликів та загроз, пов'язаних з кібервійною в Україні, та визначення заходів та рекомендацій щодо протидії цим загрозам.

Метод дослідження – аналіз інцидентів та статистичних даних. Статистичні дані про кібератаки, інциденти та іншу інформацію, що допомагає визначити типові сценарії, методи та наслідки кібервійни. Аналіз літературних джерел та наукових робіт. Огляд наукову літературу, статті, доповіді та інші джерела, що стосуються кібервійни в Україні, для отримання узагальнених знань та контексту. Вивчення конкретних кейсів кібератак або кібервійни в Україні може допомогти у розумінні конкретних сценаріїв, наслідків та заходів, що були прийняті для протидії.

ABSTRACT

Explanatory note to the master's thesis 78 p., 11 figures, 26 sources.

CYBER, WARFARE, PHISHING, PROTECTION, CYBER SECURITY, DEFACE, DDOS, OSI, NATO, OON, ES, CYBER ATTACKS, CYBER THREATS, PRIVACY, DATA, BREACHES, MALWARE, CYBERCRIME, CRITICAL INFRASTRUCTURE.

The object of the study is cyber warfare, and cyber warfare in the context of Ukraine.

The subject of the study is the analysis of cyber warfare and the development of recommendations for combating cyber threats.

The purpose of the work is to analyze the current state, challenges and threats associated with cyber warfare in Ukraine, and to determine measures and recommendations for countering these threats.

Research method – Analysis of incidents and statistical data. Statistics on cyber attacks, incidents and other information to help identify typical scenarios, methods and consequences of cyber warfare. Analysis of literary sources and scientific works. Review academic literature, articles, reports, and other sources related to cyber warfare in Ukraine for general knowledge and context. Studying specific cases of cyberattacks or cyberwar in Ukraine can help in understanding specific scenarios, consequences and countermeasures.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ВМ – Віртуальна мережа;

ІС – Інформаційна система;

МН – Машинне навчання;

ОС – Операційна система;

ПЗ – Програмне забезпечення;

ПК – Персональний комп’ютер;

СІ – Соціальна інженерія;

ІПСО – Інформаційно психологічні операції;

ARP – (Address Resolution Protocol) – Протокол визначення адрес;

DFW – (Distributed Firewall) – Розподілений міжмережевий екран;

DHCP – (Dynamic Host Configuration Protocol) – Протокол динамічної конфігурації вузла;

DNS – (Domain Name System) – Ієрархічна розподілена система перетворення імені хоста в IP-адресу;

HTTPS – (Hypertext Transfer Protocol Secure) – Протокол передачі даних;

HTML – (Hypertext Markup Language) – Мова розмітки гіпертексту;

HTTP – (Hypertext Transfer Protocol) – Протокол передачі даних;

IP – (Internet Protocol Address) – Ідентифікатор мережевого рівня;

JPEG – (Joint Photographic Experts Group) – Формат зберігання графічної інформації;

MAC – (Media Access Control) – Управління доступом до посередників;

MITM – (Man In The Middle) – Людина посередині;

PNG – (Portable Network Graphics) – Формат зберігання графічної інформації;

SMS – (Short Message Service) – Послуга обміну короткими текстовими повідомленнями в телекомунікаційних мережах;

SSL – (Secure Sockets Layer) – Рівень захищених сокетів;

TOFU – (Trust On First Use) – Режим фільтрації IP-адрес;

URL – (Uniform Resource Locator) – Уніфікований локатор ресурсів;

VLAN – (Virtual Local Area Network) – Віртуальна локальна комп'ютерна мережа;

VPN – (Virtual Private Network) – Віртуальна приватна мережа;

2FA – (Two-Factor Authentication) – Метод додаткового захисту облікового запису;

AES – (Advanced Encryption Standard) – Розширений стандарт шифрування;

DES – (Data Encryption Standard) – Стандарт шифрування інформації;

RSA – (Rivest, Shamir и Adleman) – Абревіатура від Rivest, Shamir і Adleman;

NIST – National Institute of Standards and Technology – Національний інститут стандартів і технології.

ВСТУП

В сучасному світі, де технології все більше проникають в усі аспекти нашого життя, питання кібербезпеки стає надзвичайно актуальним. Одним з найбільших викликів у цьому контексті є феномен кібервійни - нового виду конфлікту, що відбувається в цифровому просторі.

В Україні ця тема володіє особливою важливістю. У зв'язку з триваючим військовим конфліктом на сході країни, агресивною політикою Російської Федерації та після повномасштабного вторгнення, та ведення агресивної війни з боку Росії, Україна стала полем для численних кібератак, що мали на меті пошкодження її інфраструктури, економіки та соціального ладу. Відповідно, у країні створено цілу систему заходів для протидії кіберзагрозам, що включає як законодавчі акти, так і практичні рішення.

Метою даного курсового проєкту є дослідження сучасного стану кібервійни в Україні, включаючи аналіз найбільш значущих інцидентів, їх впливу на різні сфери життя країни, а також огляд діючого законодавства в області кібербезпеки. Окрім цього, проект містить розділ про перспективи розвитку кібервійни в Україні та рекомендації щодо протидії можливим загрозам.

Результати даного дослідження можуть бути корисними для спеціалістів в галузі кібербезпеки, державних службовців, науковців, а також для всіх, хто цікавиться проблемами безпеки в цифровому просторі. Крім того, вони можуть стати основою для подальших наукових досліджень у цій галузі.

1 КІБЕРВІЙНА, ТЕНДЕНЦІЇ, ВИКЛИКИ ТА ЗАГРОЗИ

1.1 Визначення та характеристика кібервійни

Кібервійна - це термін, що використовується для опису конфлікту або війни, що відбувається в кіберпросторі. Вона включає в себе стратегічно організовану серію кібератак з метою завдати шкоди інфраструктурі, економіці, національній безпеці або соціальному ладу іншої держави. Це включає в себе використання кібератак, комп'ютерного шпигунства, дезінформації, психологічного впливу та інших технік в рамках воєнних або геополітичних конфліктів.

Характеристика кібервійни включає в себе декілька ключових аспектів:

– анонімність: у кібервійні важко встановити, хто є винуватцем атаки. Це ускладнює протидію і може призвести до відсутності відповідальності за шкоду;

– швидкість дії: кібератаки можуть розгортатися з неймовірною швидкістю, що призводить до швидкого поширення шкоди;

– глобальний охоплення: завдяки глобальній природі Інтернету, кібератаки можуть впливати на цілі по всьому світу, незалежно від географічних меж;

– складність заходів протидії: важко запобігти кібератакам через складність технологічних систем та швидкість зміни технологічного ландшафту;

– висока ступінь вразливості: системи критичної інфраструктури, економічні структури, та соціальні системи стають особливо вразливими у випадку великомасштабних кібератак.

Ці особливості роблять кібервійну унікальним видом конфлікту, який вимагає спеціальних підходів до вирішення. Ці дії, як правило, виконуються

анонімно або під виглядом інших осіб або організацій, що створює унікальні виклики для встановлення винуватця та вжиття відповідних контрзаходів.

Важливо зазначити, що кібервійна може мати різні форми і масштаби, від окремих актів саботажу до широко організованих кампаній, що можуть мати серйозні наслідки для національної безпеки, економіки та суспільства країни-мети.

Кібервійни характеризуються використанням складних тактик, які включають фішинг, DDoS-атаки, шпигунські програми, злом і витік даних. Країни та організації застосовують ці методи для шпигунства, дестабілізації супротивників або навіть для прямого завдання шкоди.

Кібервійна є важливою частиною більш широкого поняття інформаційної війни і вимагає постійного розуміння та оновлення тактик та технологій для ефективної протидії.

Сучасна кібервійна ґрунтується на передових технологіях, включаючи штучний інтелект, машинне навчання, квантові комп'ютери та розширену мережеву інфраструктуру. Такі технології забезпечують високу ефективність і точність кібератак навіть на етапі, коли вони не є тотально розповсюдженими й недостатньо розвинуті, дозволяючи націлити на критичні інфраструктурні об'єкти та системи управління.

1.2 Тенденції стосовно зростання важливості кіберзлочинності та збитків від неї.

Прогнозується, що в 2023 році кіберзлочинність коштуватиме світовій економіці 8 трильйонів доларів. Прогнозується, що ця сума буде зростати до 10,5 трильйонів доларів вже до 2025 року. Аналітичні спільноти в сфері кібербезпеки порівнюють ці збитки з найбільш розвиненими економіками

таких країн як США та Китай, з їх аналізу кіберзлочинність становила би третю найбільшу економіку після цих двох країн. Важливо зауважити, що ще в 2015 році ці витрати становили 3 трильйони доларів, з чого можна зробити висновки про швидкий розвиток кіберзлочинності.

За даними Всесвітнього економічного форуму, кіберзлочинність і кібернезахищеність – нові учасники рейтингу з 10 найсерйозніших глобальних проблем щонайменше на наступне десятиліття. Посівши 8 місце, кіберзлочинність тепер стоїть пліч-о-пліч із такими загрозами, як зміна клімату та вимушена міграція.

У 2018 році Міністерство юстиції США заявило, що був зареєстрован лиш кожен сьомий кіберзлочин. У деяких країнах зареєстрований показник був ще нижчим. В 2023 році ми все ще стикаємося з ситуацією, коли менше ніж 25 відсотків кіберзлочинів, скоєних у всьому світі, надходять до правоохоронних органів.

За даними IBM, середня вартість витоку даних, включаючи втрату бізнесу, виявлення та ескалацію, сповіщення та реагування, у 2022 році становила 4,35 мільйона доларів США, що на 2,6 відсотка більше, ніж у 2021 році (4,24 мільйона доларів США). Цю цифру було отримано шляхом усереднення витрат на основі діяльності, пов’язаних з 550 організаціями, які зазнали порушень даних у 17 країнах (включно зі США, Канадою, Японією та Австралією) і 17 галузях, таких як охорона здоров’я, фінанси та енергетика[1].

1 – гостра криза постачання товарів; 2 – міждержавний конфлікт (війна); 3 – масштабна примусова міграція; 4 – зрив заходів кібербезпеки; 5 – автоматизація та зменшення робочих місць.

Рисунок 1.1 – Топ ризиків для України, по даним WEF

Далі наведена невелика вирізка з найкрупніших компаній, що були атаковані в 2023 році: Apple, Meta, Twitter, T-Mobile, Infosys, Boeing, Indian Council of Medical Research, Okta, Air Europa, 23andMe, SONY, Ontario Birth Registry, Forever 21, Duolingo, Discord.io, IBM, Police Service of Northern Ireland, Maximus, Уряд Норвегії, Roblox, PokerStars, American Airlines, UPS Canada, Mondelez (Bryan Cave), Reddit, Intellihartx, Zellis, British Airways, Apria Healthcare, Suzuki, PharMerica, Уряд США (Department of Transport), T-Mobile (друга атака), Micro-Star International (MSI), Western Digital, ChatGPT (OpenAI), US House of Representatives, Activision, Atlassian, Weee!, Sharp HealthCare, JD Sports, MailChimp, PayPal, Chick-fil-A, Slack, SevenRooms, LastPass, AirAsia Group, Dropbox, Medibank Private Ltd, Vinomofo, MyDeal, Shein (Zoetop), Toyota.

1.3 Інформаційно-психологічні операції (ІПСО)

Інформаційно-психологічні операції (ІПСО) – являють собою дії, що відповідають за передавання конкретних наративів та інформації до іноземної аудіторії з ціллю впливання на їх мотиви, почуття, критичне мислення, діяльність організацій, окремих осіб, груп та іноземних урядів. Вони являють собою важливий інструмент у сучасних військових та політичних конфліктах. Їхнє застосування може мати значний вплив на громадську думку, моральний стан військових та цивільного населення, а також на перебіг конфлікту в цілому [2].

Основна логіка полягає у тому, що люди дуже сильно чутливі до емоцій, емоції – складають значиму частину людського життя та сутності. Окрім цього в соціумі люди попадають під вплив один одного, тому якщо створити видимість того, що “вкинену” ідею підтримують люди, що розділять ваші погляди та є вашими однодумцями, то ця ідея сприймається вже з більшою довірою, ніж якщо надати просто джерело, що веде на невідому статтю, написану хтозна ким.

1.4 Історичний контекст ІПСО

ІПСО включають різноманітні тактики інформаційного та психологічного впливу, мають давню історію, сягаючи корінням в античні часи. Вони охоплюють використання пропаганди, дезінформації, символізму та інших засобів комунікації для впливу на думки та поведінку.

В античності вже можна було спостерігати приклади ІПСО, як у випадку з Троянським конем - витонченою тактикою обману, що використовувалася в

Троянській війні. Подібні тактики продовжували застосовуватись у середньовіччі, де символіка церкви та монархії, а також мистецтво ораторства використовувались для зміцнення влади та впливу на маси.

Протягом Нового часу, особливо в Наполеонівські війни, ІПСО стали більш систематизованими. Наполеон сам використовував пропаганду для підсилення свого іміджу та деморалізації опонентів.

У XX столітті, з розвитком масових медіа, ІПСО отримали новий розвиток. Під час Першої світової війни масова пропаганда та дезінформація вже широко використовувались як інструменти ведення війни. Друга світова війна ще більше підсилила роль ІПСО, де протиборчі сторони використовували пропаганду через радіо, кіно та інші медіа для підтримки воєнних зусиль та психологічного тиску на ворога, впливу на громадську думку та моральний дух як цивільного населення, так і військ ворога.

Союзні країни активно використовували засоби масової інформації, такі як радіо, кінематограф, плакати та листівки, щоб збільшити бойовий дух своїх військ та громадян, а також дестабілізувати моральний стан ворожих сил. Радіопередачі від BBC, наприклад, мали на меті надання підтримки та інформування жителів окупованих регіонів, тоді як повітряні листівки, що розкидались з літаків, були націлені на зниження бойового духу ворожих солдатів, надаючи їм інструкції для опору. Кінематографічні та графічні пропагандистські матеріали були використані для залучення підтримки серед цивільного населення.

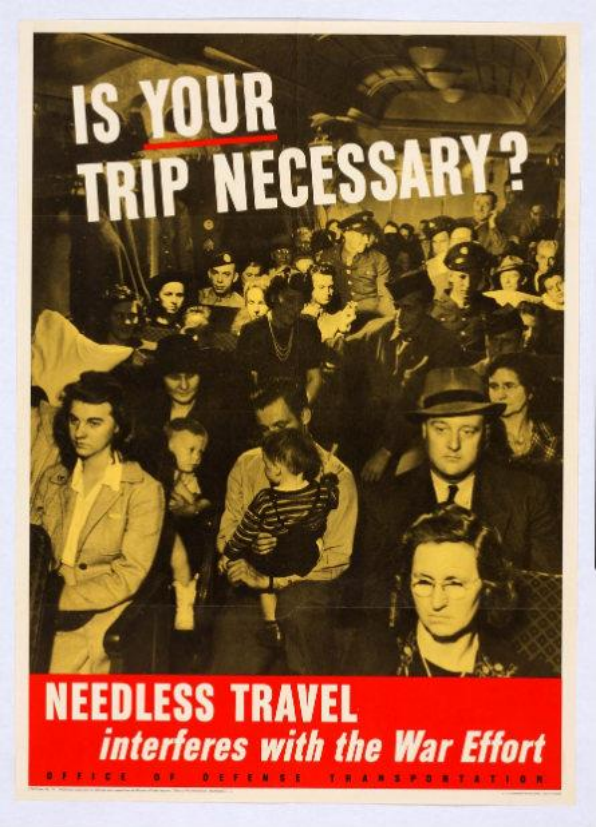

Рисунок 1.2 – Американські лозунги в рамках ІПСО [3]

З іншого боку, осьові держави, зокрема Німеччина під керівництвом Йозефа Геббельса, створили ефективну систему пропаганди через кіно, радіо та печатні видання для поширення своєї ідеології, а також зміцнення бойового духу серед населення. Японія, зосередивши увагу на поширенні своєї імперської ідеології, використовувала культурні та освітні канали для ослаблення військового потенціалу союзників, зокрема в азійсько-тихоокеанському регіоні.

Рисунок 1.3 – Німецька пропаганда в рамках ІПСО [4]

Ці операції мали суттєвий вплив на перебіг війни, оскільки вони не лише підсилювали моральний дух союзних військ, але й намагалися деморалізувати противника. Використання цих тактик сприяло загальній мобілізації громадян та підтримці воєнних дій. В результаті, інформаційно-психологічні спецоперації відіграли вирішальну роль у формуванні громадської думки та бойових діях обох сторін протистояння під час конфлікту. Вони стали суттєвим підґрунтям для подальших бойових операції, що в кінці допомогло державам союзникам перемогти у цій війні.

У сучасному світі ІПСО пристосувались до цифрової ери, використовуючи інтернет та соціальні мережі для розповсюдження інформації та дезінформації. Вони стали невід'ємною частиною так званої гібридної війни, де інформаційний простір є одним з основних полів бою.

1.5 Історичний контекст кібервійни

Перші приклади кібератак можна знайти ще в 1980-х та 1990-х роках, коли комп'ютерні системи та мережі стали все більш поширеними. Однак термін "кібервійна" почав активно використовуватися лише з початком 2000-х, коли цифрові технології стали невід'ємною частиною повсякденного життя та бізнес-процесів.

Протягом останніх десятиліть було багато випадків, які відображають зростання і розвиток кібервійн. Наприклад, відомий інцидент з "Titan Rain" в 2003 році, коли китайські хакери викрали велику кількість секретної інформації з американських комп'ютерних систем.

Ще одним значним моментом в історії кібервійн є операція "Olympic Games", здійснена США та Ізраїлем проти Ірану в 2010 році. За допомогою комп'ютерного вірусу Stuxnet, який було спеціально розроблено для цієї операції, вдалося значною мірою зіпсувати роботу іранських ядерних установок.

В Україні кібервійна стала особливо актуальною з 2014 року, коли країна стала об'єктом різноманітних кібератак. Зокрема, кібератаки на енергетичну інфраструктуру в 2015 та 2016 роках, а також кібератака "NotPetya" в 2017 році, яка завдала значних збитків не тільки Україні, але й всьому світу.

Таким чином, кібервійна стає все більш і більш важливим фактором в сучасному світі, що вимагає постійного вивчення та аналізу її історії та тенденцій розвитку.

1.6 Історія кібервійн в Україні

В контексті України, кібервійна стала особливо актуальною у контексті політичних змін та війни з Росією, які почалися з 2014 року. Відтоді Україна була предметом значної кількості кібератак з боку різних акторів, що включають державні органи та неурядові групи.

Кібератаки на енергетичну інфраструктуру. У грудні 2015 року Україна стала першою країною в світі, яка стала ціллю великомасштабної кібератаки на свою енергетичну інфраструктуру. Кібератака, здійснена групою, яку звинувачують у зв'язках з російським урядом, призвела до відключення електроенергії в декількох регіонах України.

Кібератака "NotPetya". У червні 2017 року в Україні була запущена кібератака з використанням вірусу-вимогувача NotPetya. Хоча атака була ініційована в Україні, вона швидко поширилася та вплинула на комп'ютерні системи в усьому світі, завдаючи мільярди доларів збитків.

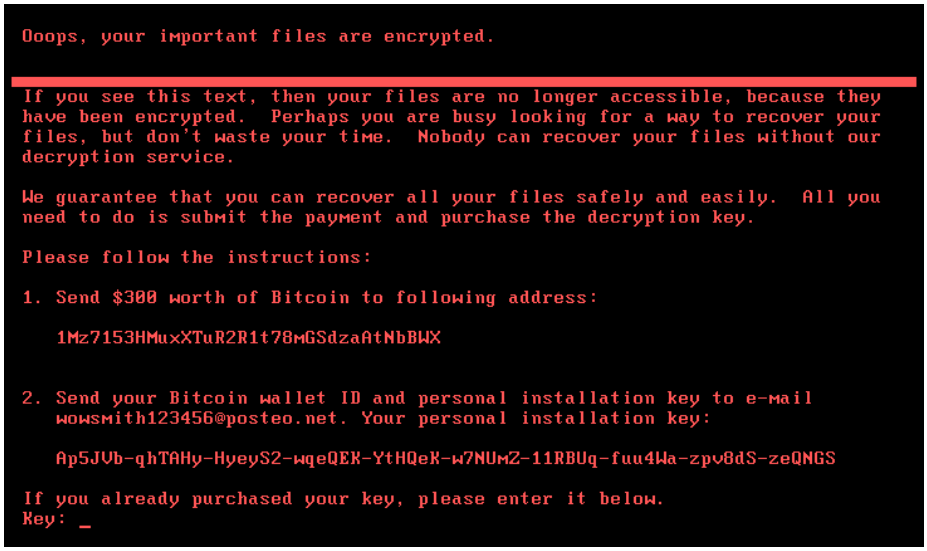

Рисунок 1.4 – Приклад атаки NotPetya [5]

Кібершпигунство та дезінформація. Україна також була предметом численних випадків кібершпигунства та дезінформаційних кампаній. Такі атаки спрямовані на підрив віри в українські демократичні інституції, втручання в політичні вибори та спричинення соціального розколу в суспільстві.

У відповідь на ці кіберзагрози, Україна вжила ряд заходів на законодавчому рівні та в сфері кібербезпеки. У 2020 році було створено Державний центр кібербезпеки, що координує заходи з кібербезпеки на національному рівні. Крім того, Україна активно співпрацює з міжнародними партнерами, включаючи ЄС і НАТО, щоб зміцнити свою кібербезпеку.

1.7 Висновки до розділу 1

Перший розділ розглядає кібервійну, визначаючи її особливості та актуальні тенденції. Кібервійна описується як конфлікт у кіберпросторі зі стратегічно організованими атаками, що мають на меті завдати шкоди інфраструктурі, економіці, національній безпеці чи соціальному порядку іншої держави.

Основні аспекти включають анонімність, швидкість дій, глобальний охоплення, складність контрзаходів, та високу вразливість критичних інфраструктур.

Розглядаються історичний контекст психологічних інформаційних операцій та зростання значення та шкоди кіберзлочинності. Окремо висвітлюється вплив та реакція на кібервійну в Україні, зокрема у зв'язку з політичними змінами та конфліктом з Росією з 2014 року.

2 АНАЛІЗ КІБЕРВІЙНИ, ПОТОЧНИЙ СТАН, РИЗИКИ ТА НАСЛІДКИ

2.1 Сучасний стан кібервійни в Україні

Сьогоднішній кіберпростір є ключовим полем битви у конфлікті з Росією. За даними 2022 року, кібератаки на Україну зросли втричі в порівнянні з попереднім роком. Пік цих атак припав на період перед великомасштабним військовим вторгненням Росії в Україну та на перші місяці після нього. За інформацією від Держспецзв'язку, основними цілями російських агресорів були державні та місцеві органи влади України, структури безпеки і оборони, а також ключові сектори економіки: фінанси, енергетика, транспорт, телекомунікації та логістика.

В ході російсько-українського конфлікту, 14 січня 2022 року було здійснено кібератаки на приблизно 22 урядові установи та 70 українських вебсайтів. На атакованих сайтах з'явився дефейс з текстом, який критикував український націоналізм польською, українською, та російською мовами. На зображенні було вказано Польщу як джерело атаки, але текст польською містив граматичні помилки, що свідчить про російське походження атаки, спрямованої на дискредитацію Польщі.

15 лютого 2022 року відбулася схожа DDoS-атака на українські сайти, що, як вважають, була здійснена Росією. Приблизно 15 банківських сайтів і сайтів з доменом gov.ua були вимкнені на 5 годин, включаючи сайти «ПриватБанку» та «Ощадбанку», а також Міноборони, Збройних сил та Міністерства реінтеграції. Міністр Михайло Федоров назвав цю атаку найбільшою в історії України, вартістю у мільйони доларів, хоча деякі експерти оцінюють її в декілька тисяч доларів.

23 лютого 2022 року, напередодні російського вторгнення, відбулися атаки на урядові та банківські сайти. Сайти Верховної Ради, Кабінету

Міністрів, Міністерства закордонних справ, СБУ та інші були пошкоджені близько 16:00. Міністерство освіти і науки закрило доступ до свого сайту, щоб запобігти атакам. Посадовці США вважають, що за атаками стоїть Росія. Компанія ESET повідомила, що атака була здійснена за допомогою вірусу HermeticWiper, створеного 28 грудня 2021 року.

У ніч та ранок 24 лютого, під час російського військового наступу, сталися кібератаки на сайт Київської обласної державної адміністрації, водночас деякі інші ресурси були вимкнені для захисту даних. Згідно з інформацією від Державної служби спеціального зв'язку та захисту інформації, на сайтах i.ua та meta.ua було розіслано велику кількість фішингових електронних листів на приватні адреси українських військових та їхніх родичів. Дослідження від Google виявило, що ця фішингова кампанія здійснювалась з території Білорусі. Також фішингові листи були відправлені українським чиновникам та польським військовим, особливо після початку прибуття українських біженців на польський кордон.

Служба безпеки України повідомила про блокування 7 тисяч ботів з Росії, які розповсюджували фальшиву інформацію про військові дії. Як заявила Служба безпеки, основними платформами для розповсюдження цієї дезінформації були Telegram, WhatsApp та Viber.

З січня 2022 року по вересень 2023 року в Україні зафіксовано майже 4000 кіберінцидентів, що в три рази більше, ніж у довоєнний період. Більшість атак координувалася Росією, яка проводила руйнівні кібератаки, проникнення в мережу та шпигунство. Також були зафіксовані активності недержавних кібердіячів, таких як проросійська хактивістська група NoName057, яка атакувала фінансовий сектор України.

2.2 Закономірність серед кібератак

Аналіз виявив, що російські ракетні удари та кібератаки на українські державні служби та компанії були скоординовані. Головними цілями цих атак стали медійні організації, засоби зв'язку, та установи, що надають підтримку Україні, включаючи логістичні та енергетичні підприємства. Наприклад, після атаки на львівську міську раду 13 травня, де були вкрадені деякі документи, 15 травня була здійснена ракетна атака на Яворівський полігон. Автори вказують на збіг географічного розташування традиційних і кібератак, що сприяє збільшенню паніки та підриву довіри до української влади.

Експерти зазначають, що основною метою атак є українські силові структури, але також постраждали цивільні стратегічні підприємства та приватні особи. Кібератаки також були спрямовані на важливі об'єкти за межами України, зокрема, майже 6 тисяч вітряних турбін у Німеччині залишились без управління через залежність від маршрутизаторів Viasat.

Підтвердженням координації кібератак і ракетних ударів є складні операції проти українських телекомпаній. До ракетних ударів російські хакери розповсюджували шкідливе програмне забезпечення DesertBlade, завдаючи збитків київським медіакомпаніям через викрадення даних та руйнування роботи. У той же день була вчинена ракетна атака на телевежу в Києві. Росія використовувала це для посилення інформаційних атак, спрямованих на поширення паніки, особливо серед літнього населення.

Російські кібератаки вражають не тільки державні установи, але й приватні компанії. Наприклад, після того як Monobank відмовився від російської версії свого додатку, банк зазнав найсильнішої атаки з часу свого заснування.

Ці кібератаки, що координуються з іншими військовими операціями, включаючи традиційні атаки на фронті та пропагандистські дії, мають велике

значення. Яскравий приклад - серія атак на енергетичну інфраструктуру, що підсилювалася ракетними ударами.

Автори дослідження підкреслюють, що світ веде першу повномасштабну кібервійну, де бойові дії відбуваються не тільки на землі та в повітрі, а й у кіберпросторі, який вже вважається окремим театром воєнних дій в країнах НАТО та Україні. Зростання цифровізації світу збільшує потенційну небезпеку кібератак. Тому ворог застосовує терор у всіх можливих сферах.

2.3 Атаки IT-армії України

Як відповідь на попередні кібератаки, була анонсована ініціатива створення IT-армії, яка об'єднає фахівців з різних сфер для протидії дезінформації в Інтернеті та проведення атак на російські веб-сайти. Ініціатором цього проекту є Єгор Аушев, розробник платформ CyberUnit.Tech, Cyber School та Hacken.io [14]. Він запропонував ідею формування кіберармії на базі добровольців, ідея якої отримала підтримку від Міністра цифрової трансформації України Михайла Федорова. Незабаром після цього десятки російських банківських, державних, новинних веб-сайтів та інших ресурсів зазнали атак. Деякі російські телеканали навіть почали транслювати українські пісні[17].

На початку березня 2022 року українські хакери оголосили про успішні кібератаки, які знешкодили важливі інформаційні системи російських окупантів. Незважаючи на протидію з боку російських кібервійськ, українські хакери завдали серйозної шкоди ворожій інформаційній інфраструктурі. Особливо, 24 лютого була заблокована система "Систематики" — автоматизована система "Вибори", яку використовував Путін для фальсифікації виборів. Також були знешкоджені системи електронного

документообігу окупаційної влади в Криму, Донецьку та Луганську. Інформація про тих, хто підтримував окупацію, була передана у правоохоронні органи. 25 лютого була знищена система управління Федерального казначейства РФ та її резервні копії. Російська влада приховує факт та наслідки українських кібератак, намагаючись підтримувати ілюзію "непереможності" своєї армії.

Звісно, Україна зазнає більше атак від російських хакерів та спецпідрозділів ФСБ та армії, ніж інші країни. У перші три дні війни кібератаки на український державно-військовий сектор зросли на 196% у порівнянні з періодом до повномасштабного вторгнення. Рекордом росіян стало 275 DDoS-атак за день. Однак це значно менше, ніж кількість атак, які Україна відправляє у відповідь.

У 2022 році українські кіберсили здійснили понад мільйон DDoS-атак на російську інфраструктуру. Найдовша з цих атак тривала 29 днів. Після російського вторгнення в Україну, Росія стала головною метою для IT-фахівців з усього світу. Кількість DDoS-атак на російську інфраструктуру в 2022 році зросла на 700% порівняно з попереднім роком.

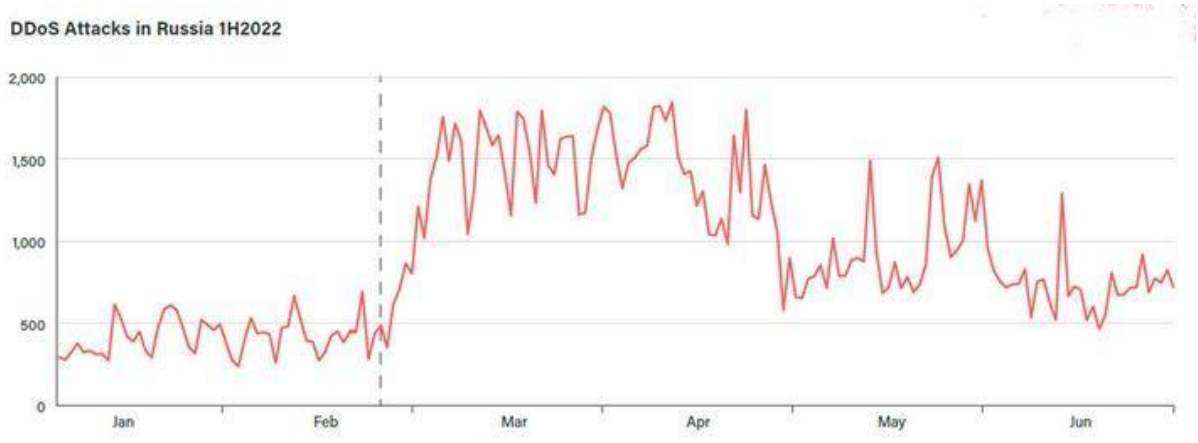

Рисунок 2.1 – Динаміка DDoS-атак на РФ у першій половині 2022 року за даними Netscout [6]

В 2022 році було зареєстровано 1 255 573 DDoS-атаки на об'єкти російської інфраструктури, що віднесло Росію на четверте місце в світовому рейтингу країн, які найчастіше стають мішенями кібератак. Лідерами цього списку залишаються Індія та Китай.

Головними напрямками, на які сконцентрували свою увагу українські хакери, стали фінансова сфера — 28% від усіх атак, телекомунікації — 14%, державний сектор — 14% та роздрібна торгівля — 12%. Українська IT-армія використовує креативний підхід у своїх атаках. Більшість з них були сплановані з урахуванням конкретних дат, щоб максимізувати шкоду. Наприклад, вони часто блокували комп'ютерні мережі великих компаній в кінці місяця або кварталу, коли підприємства мають подавати фінансові звіти та іншу важливу документацію.

Спеціалісти IT-армії часто підходять до виконання задач креативно. Наприклад, ось так виглядали сайти ФСІН, Мінкульту, Міненерго, Росатома та ще низки російських інституцій після атак кібервійська 8 березня:

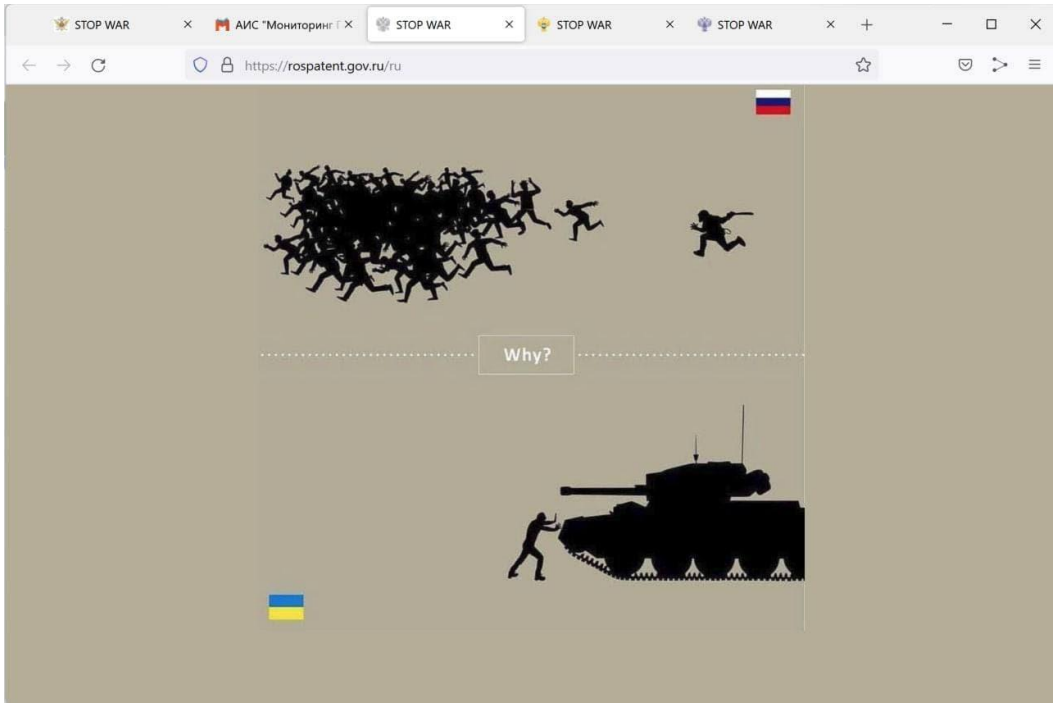

Рисунок 2.2 – Результат атак IT армії України на російські сервіси [7]

2.4 Кібератаки рівня L7

У ранній стадії російсько-українського кіберконфлікту переважно використовувались атаки 3-го та 4-го рівня — з метою виведення з ладу інфраструктури. Такі атаки перевантажували мережі та програми, роблячи їх нездатними до нормального функціонування через обмежену пропускну спроможність. Однак сучасний етап кібервійни характеризується більш витонченими методами. Учасники зараз активно використовують атаки 7-го рівня, які є інтелектуальними та цілеспрямовано шукають слабкі місця в кіберінфраструктурі, блокуючи її або серйозно порушуючи її роботу на тривалий час. Атаки рівня L7, або атаки рівня застосування, відносяться до найвищого рівня в моделі OSI (Open Systems Interconnection), яка описує різні рівні взаємодії мережевих протоколів. Модель OSI складається з семи рівнів, від фізичного рівня (рівень 1) до рівня застосування (рівень 7).

Атаки рівня застосування, або атаки рівня L7, спрямовані на процеси та протоколи, які використовуються програмами та службами для здійснення мережевих взаємодій. Це можуть бути веб-сайти, бази даних, поштові сервери, системи управління контентом (CMS) тощо [8].

Однією з найвідоміших атак рівня L7 є атаки DDoS (розподілені відмови в обслуговуванні), коли атакуючий збільшує обсяг мережевого трафіку або запитів до певного сервісу або веб-сайту, намагаючись перевантажити його та викликати збої в роботі.

Ці атаки особливо небезпечні, оскільки вони можуть використовуватися для блокування важливих сервісів або навіть викрасти конфіденційні дані. Боротьба з атаками рівня L7 вимагає складних та просунутих методів захисту, які зазвичай включають ідентифікацію та блокування підозрілого трафіку, використання систем захисту від DDoS атак, інтелектуального аналізу трафіку та додаткових шарів аутентифікації.

2.5 Виклики та загрози кібервійни

У сучасному світі, де технології розвиваються неймовірно швидко, концепція кібервійни стає все більш актуальною та загрозливою. Одним із основних викликів кібервійни є її прихований характер. На відміну від традиційних військових конфліктів, кібератаки часто відбуваються анонімно, що ускладнює визначення відповідальності та реагування на них. Це створює значні проблеми для національної безпеки та міжнародних відносин, оскільки визначення винуватця атаки часто перетворюється на складну задачу.

Ще однією серйозною загрозою є широкий спектр потенційних цілей. Кібератаки можуть бути спрямовані на важливі державні установи, такі як енергетичні системи, транспортні мережі, фінансові інститути, а також на приватний сектор і навіть на окремих осіб. Це створює велику кількість потенційних "фронтів", де може бути застосована кібервійна.

Крім того, швидкий розвиток технологій постійно змінює пейзаж кібервійни, вносячи нові інструменти та методики в арсенал як нападників, так і захисників. Це означає, що для ефективного захисту необхідно постійно адаптуватися та оновлювати свої кіберооборонні стратегії.

В цілому, кібервійна представляє собою складний виклик, який вимагає уваги, ресурсів та співпраці на міжнародному рівні, щоб протидіяти цій загрозі та мінімізувати її негативні наслідки для глобальної стабільності та безпеки.

2.5.1 Загроза національній безпеці

Кібервійна може стати серйозною загрозою для національної безпеки країни. Це стосується не тільки можливості атак на критичну інфраструктуру (енергетику, транспорт, комунікації тощо), але і розповсюдження дезінформації, спрямованої на підрив стабільності в країні. Кібератаки можуть бути спрямовані на критичну інфраструктуру країни, таку як енергетичні мережі, водопостачання, системи транспорту та комунікації. Ці системи є життєво важливими для функціонування країни, і їх відмова може мати катастрофічні наслідки.

У військових конфліктах, кібератаки можуть бути використані як додатковий інструмент для досягнення стратегічних цілей. Наприклад, вони можуть бути використані для знешкодження оборонних систем, саботажу військової інфраструктури або викрадення конфіденційної інформації.

Кібервійна також може включати використання цифрових технологій для розповсюдження дезінформації та пропаганди. Це може підривати довіру громадян до уряду та інших інституцій, спричиняти соціальні розбрати та суспільну нестабільність.

Кібервійна також може включати викрадення конфіденційної інформації, що може підривати національну безпеку. Це може включати державні секрети, відомості про оборонну технологію, даних про економіку країни та інше.

2.5.2 Економічні втрати

В результаті кібератак можуть виникнути значні економічні втрати. Це може включати втрату даних, витрати на відновлення системи, втрату прибутку внаслідок перебоїв в роботі, а також втрату довіри клієнтів.

Наприклад, 2020 року оцінка непрямих втрат світової економіки від кібератак становить близько 1 трильйона доларів. За 2021-й кількість атак зросла на 15%, а до 2025 року втрати від кібератак для світової економіки оцінюють у понад 10 трильйонів доларів. Це більше, ніж теперішні втрати від коронавірусної кризи та повномасштабного вторгнення рф разом.

Використання кіберзброї — чи не останній засіб ефективного спротиву в умовах тотальної переваги супротивника. Прикладом цьому слугують успішні кібератаки в Білорусі на залізничну систему. За доповіддю ООН, дохід від кібератак навіть дозволяє фінансувати ядерну програму Північної Кореї.

2.5.3 Порушення приватності

Атаки, спрямовані на крадіжку даних, можуть призвести до порушення приватності окремих осіб. Це може мати серйозні наслідки, включаючи ідентифікаційне шахрайство та інші форми злочинності.

Однією з найпоширеніших тактик у кібервійні є шпигунство або збір інформації. Це може включати в себе крадіжку особистої інформації, такої як імена, адреси, номери телефонів, фінансові дані та інше. Зібрана інформація може бути використана для різноманітних цілей, включаючи шахрайство, шантаж, провокацію соціальних рухів або підготовку до фізичних атак.

Зловмисники можуть використовувати взлом для незаконного доступу до приватних систем або мереж, використовуючи їх для крадіжки, зміни або видалення даних. Такий взлом може включати в себе комп'ютери, мобільні пристрої, рахунки в соціальних медіа, електронну пошту та інші електронні системи.

У контексті кібервійни, порушення приватності також можуть бути пов'язані з розповсюдженням дезінформації або фальшивих новин. Зловмисники можуть використовувати викрадену інформацію для створення і розповсюдження неправдивої інформації, що може викликати соціальну нестабільність або змінювати громадську думку.

2.5.4 Втрата довіри до інституцій

Кібератаки на державні інституції можуть підривати довіру громадян до цих організацій. Це особливо актуально в періоди виборів, коли довіра до системи є важливою.

Втрата довіри до інституцій через кібервійну є ще одним наболілим питанням, що виникає в результаті масових кібератак. Якщо урядові органи, банки, медичні установи, освітні заклади та інші інституції не зможуть ефективно захистити свої мережі та системи від кібератак, громадяни можуть почати втрачати довіру до них.

Втрата довіри може мати далекосяжні наслідки. Наприклад, якщо громадяни втратять довіру до банківських систем через кібератаки, вони можуть відмовитися від використання банківських послуг, що може призвести до фінансової нестабільності. Якщо громадяни втратять довіру до медичних установ, вони можуть не звертатися за необхідною допомогою або не довіряти медичній інформації, що може мати негативні наслідки для здоров'я громадян.

Крім того, втрата довіри може підірвати довіру до уряду та інших громадських інституцій. Це може призвести до політичної нестабільності, а також до збільшення недовіри та апатії громадян.

У контексті України, де кібератаки є поширеними, втрата довіри до інституцій може бути серйозною проблемою. Тому захист від кібератак та зміцнення кібербезпеки є важливими для збереження довіри громадян до цих інституцій.

2.5.5 Потреба в постійному оновленні технологій безпеки

Внаслідок швидкого розвитку технологій, нових видів атак та методів захисту, є постійна потреба в оновленні технологій безпеки та підвищенні кваліфікації фахівців.

Всупереч постійному прогресу в області кібербезпеки, технології швидко старіють у зв'язку з безперервним розвитком методів та тактик кібервійни. Зловмисники постійно вдосконалюють свої навички та використовують все більш витончені та непередбачувані методи нападу. Це ставить під загрозу не тільки великі організації та уряди, але й окремих користувачів.

Потреба в постійному оновленні технологій безпеки виникає як реакція на цю постійну зміну. Це означає, що компанії, уряди та індивідуальні користувачі повинні не тільки інвестувати в найновітніше обладнання та програмне забезпечення для захисту своїх систем, але також постійно оновлювати свої знання та навички для захисту від нових загроз.

Також важливо зрозуміти, що технології безпеки не обмежуються тільки антивірусним програмним забезпеченням та брандмауерами. Вони також

включають різні технології, такі як шифрування, аутентифікація, моніторинг мережі, системи захисту від вторгнення та ін.

Що стосується України, країни, що стикається з постійними кібератаками, потреба в оновленні технологій безпеки є особливо актуальною. Для забезпечення ефективного захисту від кібервійни, український уряд, компанії та громадяни повинні бути готові до швидкого оновлення своїх технологій безпеки відповідно до змінюваних умов та загроз.

2.5.6 Значення криптографії для захисту даних та інформаційних систем.

Криптографія — ключовий елемент у захисті цифрових даних. Вона не тільки маскує конфіденційну інформацію, але й є ефективним захистом від хакерських атак. Це дає змогу забезпечувати безпеку важливих даних, які пересилаються або зберігаються.

Завдяки криптографії, можливо захистити особисті дані та забезпечити безпечне виконання транзакцій. Ця технологія стала необхідністю у сучасних системах безпеки, адже вона допомагає захищати відомості про особу та інші конфіденційні дані [9].

Криптографія також сприяє верифікації даних та документів, допомагаючи запобігати їх фальсифікації. Це важливо для створення довіри в цифровому світі, де аутентичність інформації є ключовою.

Технологія криптографії перетворює дані в незрозумілий формат, який неможливо прочитати без спеціального ключа. Це комплексний процес, що включає застосування різних методів шифрування, які роблять інформацію недоступною для несанкціонованого доступу.

Економічна ефективність криптографії полягає у забезпеченні безпеки даних за помірні кошти. Вона використовує такі методи, як симетричні

алгоритми, де один і той же ключ застосовується для шифрування та розшифровки, забезпечуючи тим самим високий рівень безпеки при збереженні конфіденційності даних.

Ці аспекти криптографії роблять її незамінною у захисті цифрових інформаційних систем від зовнішніх загроз, гарантуючи конфіденційність, цілісність даних та безпеку в цілому.

2.5.7 Криптографічні методи і алгоритми

У кібервійськових операціях важливе значення має застосування криптографічних методів для захисту конфіденційної інформації. Такі методи включають:

– Triple DES це сучасний стандарт у криптографії. Triple DES підвищує безпеку через унікальний процес симетричного шифрування, який шифрує дані тричі, використовуючи три 56-бітні ключі, що ефективно створює 168-бітне шифрування.

– Twofish Cipher походить від Blowfish, Twofish - це симетричний шифр, підходящий для менших процесорів. Він забезпечує постійний процес шифрування з 16 раундами, незалежно від розміру ключа, пропонуючи гнучкість у налаштуванні ключа і швидкості шифрування.

– Advanced Encryption Standard (AES): AES вирізняється своїм підходом блокового шифру, шифруючи дані у великих блоках, а не малих партіях. З такими варіантами, як AES-256, AES-192 та AES-128, він забезпечує кілька раундів шифрування, підвищуючи безпеку конфіденційних даних.

– RSA Algorithm: Ця асиметрична криптографічна техніка, названа на честь її творців Рівеста, Шаміра та Адельмана, використовує два ключі –

приватний і публічний. Сила RSA полягає у великих розмірах ключів, часто від 1024 до 2048 біт, що робить її надійним вибором для передачі даних через незахищені мережі.

Ці криптографічні методи є необхідними у кібервійськових операціях, пропонуючи надійний захист від витоків даних і забезпечуючи безпечне спілкування у ворожих цифрових ландшафтах.

2.5.8 Стандарт Triple DES

Triple DES, також відомий як TDEA або Triple DEA, це симетричний блоковий шифр, який застосовує алгоритм шифру DES тричі до кожного блоку даних. Запропонований у 1978 році, цей метод шифрування використовує два або три 56-бітні ключі для збільшення безпеки. Triple DES був стандартизований у різних документах, включаючи RFC 1851, ANSI ANS X9.52-1998, FIPS PUB 46-3, NIST Special Publication 800-67 Revision 2, та ISO/IEC 18033-3:2010.

Triple DES працює за допомогою "пакету ключів", який складається з трьох ключів DES. Шифрування включає три етапи: шифрування з K1, дешифрування з K2, потім знову шифрування з K3. Така схема шифрування посилює алгоритм та забезпечує зворотну сумісність з DES.

Але в 2018 році NIST відмовився від цього алгоритму через його низький рівень безпеки, наразі на заміну йому прийшов AES[10].

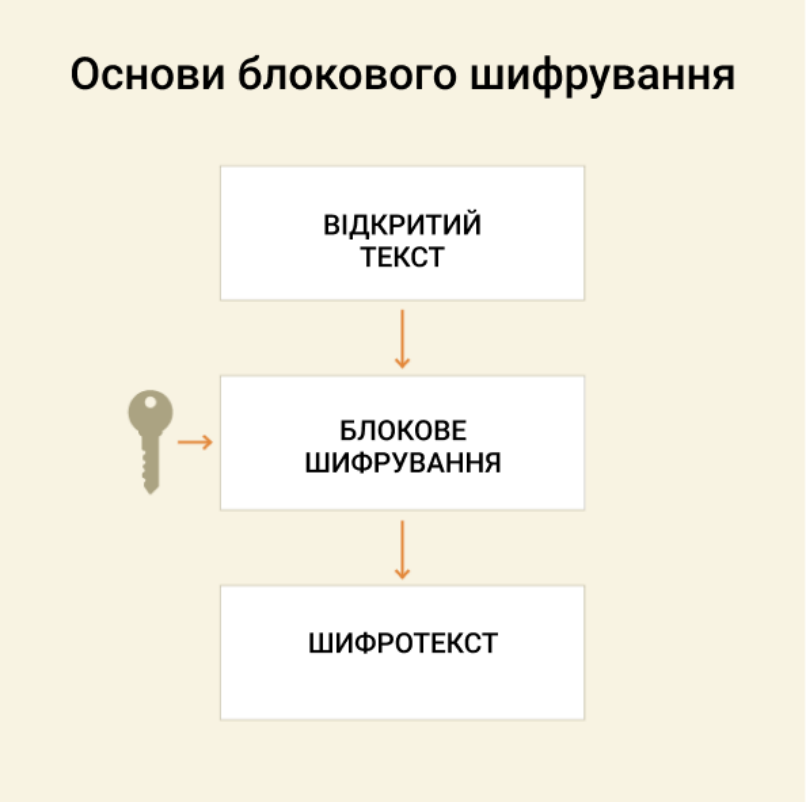

Рисунок 2.3 – Основи блокового шифрування

Існує три варіанти ключів для Triple DES. Найбезпечніший варіант використовує три незалежні ключі. Triple DES є вразливим до атак типу "meet-in-the-middle" і атак зіткнення блоків, особливо при шифруванні великих обсягів даних з одним ключем.

Triple DES був широко використаний в промисловості електронних платежів і в ранніх версіях програмного забезпечення Microsoft, але з часом його використання зменшилося через зростання популярності більш безпечних алгоритмів, таких як AES.

2.5.9 Twofish Cipher

Twofish - це симетричний блоковий шифр з блоком 128 біт і розмірами ключів до 256 біт, розроблений для конкурсу AES. Його унікальні особливості включають ключозалежні S-блоки та складний розклад ключів, з дизайном, натхненним його попередником, Blowfish. За швидкістю Twofish був порівнянний з Rijndael.

Рисунок 2.4 – Приклад Twofish шифрування

Розроблений командою на чолі з Брюсом Шнайєром, Twofish не запатентований і доступний для вільного використання. Хоча його використання менш поширене, ніж Blowfish, він відомий своєю гнучкою продуктивністю в різних застосуваннях. Twofish підтримує компроміси між

часом та простором у своїй реалізації, збалансовуючи швидкість і вимоги до пам'яті [11].

У сфері розвідки, дрони та обладнання для спостереження, які є невід'ємною частиною сучасної війни, часто обробляють високочутливі дані. Шифрування цих даних Twofish під час передачі гарантує, що вони можуть бути доступні лише авторизованим особам, забезпечуючи таким чином оперативну безпеку. Більше того, у наземних операціях безпечний обмін повідомленнями є важливим для координації та безпеки військовослужбовців. Впровадження шифрування Twofish для повідомлень, які обмінюються між підрозділами, може захистити важливу інформацію про переміщення військ та тактичні плани від перехоплення ворогом.

2.5.10 Advanced Encryption Standard

AES, спочатку відомий як Рейндаель, був затверджений як стандарт шифрування NIST у 2001 році. Розроблений Жоаном Даєменом та Вінсентом Райменом, AES замінив DES, пропонуючи підвищену безпеку. Він використовує симетричний ключ для шифрування та розшифрування.

На відміну від DES, AES базується на мережі заміщення-перестановки, не використовуючи мережу Фейстеля. AES працює з блоками розміром 128 біт і має варіанти ключів 128, 192 або 256 біт, що визначає кількість раундів шифрування. Шифрування включає такі етапи, як нелінійне заміщення (SubBytes), транспозиція (ShiftRows), лінійне змішування (MixColumns) та додавання ключа (AddRoundKey) [12].

AES залишається ефективним від існуючих атак, забезпечуючи захист даних, зашифрованих за допомогою AES.

2.5.11 RSA алгоритм

RSA (Rivest–Shamir–Adleman) є одним з найвідоміших алгоритмів шифрування з відкритим ключем. Він використовується для безпечного шифрування даних та цифрового підпису. RSA ґрунтується на математичній складності факторизації великих цілих чисел. Це робить його стійким до багатьох типів криптографічних атак, особливо коли використовуються великі ключі (наприклад, 2048 біт або більше).

Однак, RSA вимагає значно більше обчислювальних ресурсів, ніж симетричні шифри, як-от AES. Також зростання потужності квантових комп'ютерів у майбутньому може створити ризики для алгоритмів, які, як RSA, покладаються на факторизацію великих чисел. Тому важливо вибирати алгоритми шифрування, виходячи з поточних вимог до безпеки та розміру даних, які потрібно захистити [13].

2.5.12 Використання криптографічних методів у кібервійськових операціях.

Використання криптографічних методів у кібервійськових операціях є критично важливим для забезпечення безпеки даних та комунікацій. Криптографія дозволяє захистити конфіденційність інформації, забезпечує аутентичність повідомлень, захищає від несанкціонованого доступу та допомагає у запобіганні маніпуляціям з даними. Під час війни, вони використовуються для шифрування комунікацій, захисту даних на серверах та мобільних пристроях, а також для забезпечення безпеки дистанційно керованих систем, таких як безпілотні літальні апарати.

Використання криптографічних алгоритмів, як-от AES, RSA, Twofish та Triple DES, має ключове значення для забезпечення безпеки комунікацій та даних. AES, з його високою стійкістю та ефективністю, ідеально підходить для захисту важливих військових комунікацій та розвідувальних даних, переданих через БПЛА. RSA ефективний для цифрових підписів та аутентифікації. Хоча Twofish та Triple DES мають свої обмеження у порівнянні з AES, вони можуть бути використані у певних ситуаціях, де потрібна гнучкість у реалізації або де ще не відбувся перехід на сучасніші технології шифрування. Вибір шифрування повинен враховувати баланс між безпекою, продуктивністю та сумісністю з обладнанням.

Криптографічне шифрування окрім захисту власних комунікаційних систем та тощо, також використовують для сокриття власних кібератак, одним з прикладів може бути Stuxnet, який являє собою вірус, що був створен для кібератак на ядерні об'єкти Ірану. Складні криптографічні шифрування використовувались для унеможливлення своєї присутності та діяльності від захисних систем.

2.6 Розвиток та використання новітніх технологій у кібервійнах

Розвиток новіших технологій та їх застосування у сфері кібервійн є ключовою темою у сучасному цифровому світі. З огляду на збільшення залежності від цифрових систем і широке використання інтернету у всіх аспектах життя, кібервійни стали значущим феноменом. Кібервійна означає використання комп'ютерних технологій та мереж для здійснення агресивних дій проти інформаційних систем опонента, включаючи кібершпіонаж, поширення фальшивої інформації, блокування інфраструктурних систем, а

також безпосередні кібератаки на критично важливі державні та військові об'єкти.

Прогрес у сферах штучного інтелекту, машинного навчання, блокчейну та квантових обчислень відкриває нові горизонти для кібервоєнних дій. Штучний інтелект можна використовувати для автоматизації кібератак та оборонних операцій, а також для аналізу великих даних для виявлення слабких місць у системах супротивника. Машинне навчання допомагає створювати більш складні методи взлому систем безпеки. Технологія блокчейну може забезпечувати високий рівень безпеки та анонімності в кібероперація́х, тоді як квантові обчислення в майбутньому можуть змінити основи криптографічного захисту.

Ці технології, разом із своїми перевагами, також мають потенційні ризики. Вони можуть бути використані не лише державними структурами, але й недержавними учасниками, включаючи терористичні угруповання та кіберзлочинців. Це створює складні виклики для глобальної безпеки та стабільності.

З огляду на це, міжнародна спільнота повинна визначити правила і норми, які регулюватимуть кібервійни та використання передових технологій у військових цілях. Мова йде не тільки про юридичні питання, але й про розробку етичних принципів та стандартів поведінки у кіберпросторі. Крім того, уряди та приватний сектор мають спільно працювати над підвищенням своїх кібероборонних можливостей і розвивати культуру кібербезпеки серед населення.

Кібервійни, що відбуваються в цифровому віці, стали ключовим аспектом глобальної безпеки та геополітики. Цей новий вид конфлікту використовує революційні технології, які розширюють можливості для проведення військових та шпигунських операцій. У цьому контексті, розуміння того, як сучасні технології, такі як штучний інтелект, машинне навчання, блокчейн та інтернет речей, впливають на динаміку кібервійн, є

життєво важливим. Вони змінюють традиційні підходи до ведення війни та ставлять нові виклики перед урядами, військовими та корпораціями у всьому світі. Ось головні аспекти цієї динамічної і швидко розвиваючої області:

– штучний інтелект і машинне навчання: ці технології відіграють критичну роль у розвитку кібервоєнних стратегій. Вони використовуються для автоматизації виявлення вразливостей в системах безпеки, удосконалення методів кібератак та покращення засобів кіберзахисту. Алгоритми машинного навчання здатні аналізувати величезні обсяги даних, щоб виявляти тенденції та передбачати потенційні атаки.

– розповсюдження дезінформації: цифрові платформи, соціальні мережі та інші онлайн інструменти використовуються для масового розповсюдження дезінформації, спрямованої на дестабілізацію суспільств та маніпулювання громадською думкою. Такі техніки стають основною частиною гібридної війни, де інформаційні атаки стають такими ж важливими, як і традиційні військові дії.

– квантові обчислення: хоча ця технологія ще перебуває на ранньому етапі розвитку, вона має потенціал радикально змінити кібербезпеку. Квантові комп'ютери можуть в майбутньому розшифровувати навіть найміцніші криптографічні системи, що поставить нові виклики перед розробниками захисних кібертехнологій.

– блокчейн: блокчейн використовується не тільки у фінансовому секторі, але й у кібербезпеці. Його децентралізована природа і стійкість до маніпуляцій роблять його корисним для забезпечення безпеки даних та ускладнення кібератак.

– інтернет речей (IoT): з розвитком IoT, все більша кількість пристроїв підключаються до інтернету, що розширює площину потенційних кібератак. Ці пристрої часто мають вразливості у безпеці, які можуть бути використані для здійснення масових кібератак або створення ботнетів.

– кіберзахист і відповідні заходи: на тлі зростаючих кіберзагроз, уряди та організації по всьому світу активно працюють над розробкою більш ефективних систем кіберзахисту. Це включає в себе впровадження розширених технологій шифрування, створення спеціалізованих кібероборонних команд та розробку стратегій для протидії кібератакам.

Разом, ці елементи утворюють складний та багатогранний ландшафт кібервійн, де технології постійно еволюціонують, а стратегії та тактики адаптуються до нових викликів та можливостей. Важливо, що держави та організації визнають ці зміни та активно працюють над розвитком та впровадженням нових підходів до кібербезпеки та оборони.

2.6.1 Майбутні тренди у кібербезпеці та напрямки її розвитку

Кіберзагрози стають все більш витонченими та шкідливими, створюючи безпрецедентні виклики для організацій, урядів та індивідуальних користувачів. У цьому контексті розуміння майбутніх трендів та напрямків розвитку кібербезпеки є ключовим для підготовки та адаптації до нових викликів, повищаючи рівень гнучкості та швидкості реагування на майбутні загрози, з якими нам належить зіткнутися. Це включає в себе не тільки розробку нових технологічних рішень для захисту інформації, але й формування сильної свідомості про кібербезпеку серед всіх користувачів інтернету [15].

Майбутні тренди і напрямки розвитку кібербезпеки охоплюють кілька ключових аспектів:

– Штучний інтелект та машинне навчання: Використання AI і ML у кібербезпеці дозволяє більш ефективно виявляти та реагувати на кіберзагрози, аналізувати великі обсяги даних та передбачати потенційні

атаки. Наприклад, алгоритми машинного навчання здатні аналізувати типову активність мережі та виявляти незвичайні відхилення, які можуть свідчити про втручання зловмисників. Крім того, AI і ML сприяють розвитку методів прогнозування в сфері кібербезпеки, дозволяючи організаціям антиципувати та підготуватися до можливих кібератак. Це стає все більш важливим в контексті постійної еволюції кіберзагроз, де традиційні методи часто виявляються недостатніми перед обличчям нових тактик кіберзлочинців. Проте, інтеграція AI та ML у системи кібербезпеки також створює нові виклики, включаючи необхідність забезпечення якісних даних для навчання алгоритмів та ризик використання цих же технологій зловмисниками для розробки більш складних атак. Таким чином, паралельно з впровадженням AI і ML, важливим є також розвиток заходів для протидії можливим маніпуляціям і адаптації систем кібербезпеки до нових умов;

– Захист Інтернету речей (IoT): з ростом популярності IoT-пристроїв з'являється потреба в більш суворих мірах безпеки для захисту цих пристроїв та збереження конфіденційності даних. Важливо впроваджувати регулярні оновлення програмного забезпечення для усунення вразливостей, забезпечувати захист від фізичного доступу до пристроїв, а також використовувати надійне шифрування даних для запобігання їх витоку. Ці заходи допомагають створити більш безпечне середовище для IoT-пристроїв, які все більше інтегруються в повсякденне життя людей, забезпечуючи їх зручність та підвищуючи ефективність різних процесів;

– Блокчейн для безпеки: блокчейн може забезпечити вищий рівень безпеки завдяки своїй децентралізованій та прозорій природі, що може бути корисно для захисту від шахрайства, витоків даних та інших кіберзагроз. Крім того, застосування блокчейну у сфері кібербезпеки відкриває нові можливості для створення надійних систем ідентифікації та аутентифікації. Це може значно знизити ризики пов'язані з крадіжкою ідентифікаційних даних та несанкціонованим доступом до конфіденційної інформації.

Використання розподілених реєстрів у блокчейні дозволяє створювати міцніший механізм верифікації, який є важким для порушення зловмисниками. Такий підхід може бути особливо ефективним у промислових секторах, де важливо забезпечити безпечний обмін даними між різними сторонами;

– Більш складні кібератаки: очікується, що кіберзлочинці будуть використовувати більш витончені методи, такі як глибоке підроблення (deepfakes), AI-підсилені атаки та цілеспрямовані фішингові кампанії;

– Приватність даних і регулювання: зростаюча увага до приватності даних та вимоги до їх захисту, такі як GDPR в ЄС, спонукатимуть компанії до посилення своїх політик та практик кібербезпеки;

– Об'єднання кібербезпеки і фізичної безпеки: охорона критичної інфраструктури та інтеграція кібербезпеки з фізичними заходами безпеки стануть ще більш важливими;

– Освіта та свідомість: підвищення обізнаності про кібербезпеку серед працівників та загальної публіки буде ключовим у запобіганні кіберзагрозам.

2.7 Аналіз міжнародного права та його застосування до кібервійн

Сучасне міжнародне право відстає від стрімких технологічних змін, особливо з урахуванням загроз, які створюють сучасні технології, такі як квантові комп'ютери. Хоча міжнародні зусилля спрямовані на визначення кібероперацій в контексті озброєних конфліктів, існує значна невизначеність щодо регулювання кібервійни, особливо з огляду на питання атрибуції

кібератак, їхнього віднесення до військових або цивільних дій, а також необхідність розрізнення між кібератаками та кібершпіонажем.

Дискусії щодо кібервійни виникали з міжнародного права озброєних конфліктів. Після кібератак на Естонію в 2007 році міжнародна спільнота почала серйозніше обговорювати кіберпростір як арену війни. Це призвело до створення Таллінського посібника з міжнародного права, яке застосовується до кібервійни. Тим не менш, міжнародне співтовариство не впровадило єдиний правовий фреймворк для регулювання кібератак та кібервійни. Існує дебат щодо того, чи слід застосовувати існуючу правову структуру до кіберконфліктів, чи потрібен новий правовий фреймворк.

Існує декілька підходів до аналізу сили кібератак, включаючи інструментальний підхід, який фокусується на техніці, використаній у атаці, цільовий підхід, який зосереджується на мішені атаки, та підхід, заснований на наслідках, який орієнтується на реперкусії та результати атаки. Останній підхід є найпопулярнішим і включає оцінку реальних наслідків атаки.

Важливим аспектом є також неможливість точного встановлення джерела кібератаки, що ускладнює застосування концепції самооборони, передбаченої статтею 51 Уставу ООН, та збільшує ризик неправильно спрямованої реакції [16].

Зрештою, глобальні зусилля щодо формування права кібервійни будуть малоефективними, якщо великі військові держави, особливо США та Китай, не увійдуть у обов'язкову міжнародну угоду, що обмежує їхні можливості ведення кібервійни.

2.7.1 Приклади міжнародних угод та конвенцій, що регулюють кіберконфлікти

У контексті постійно зростаючої значущості кіберпростору як арени глобальних взаємодій та конфліктів, розгляд міжнародних угод та конвенцій, які регулюють кіберконфлікти, стає ключовим аспектом забезпечення міжнародної безпеки та стабільності. Ця підтема акцентує увагу на існуючих міжнародних правових рамках, які адресують виклики, пов'язані з кібератаками та кібервійною, а також обговорює їхню адекватність та ефективність у контексті швидкого розвитку кібертехнологій. Ми розглянемо як вже існуючі міжнародні угоди, так і поточні ініціативи, спрямовані на розвиток та удосконалення міжнародного правового поля у цій сфері. Цей аналіз дозволяє оцінити, наскільки міжнародне співтовариство готове відповідати на виклики, що виникають у кіберпросторі, та які кроки необхідні для зміцнення правових механізмів забезпечення кібербезпеки.

Конвенція Ради Європи про кіберзлочинність (2001). Відома також як Будапештська конвенція, ця угода є першою міжнародною спробою вирішити проблему кіберзлочинності, створюючи загальний правовий фреймворк і сприяючи міжнародному співробітництву.

Конвенція зосереджується на таких питаннях, як незаконний доступ, перехоплення даних, шкідливе програмне забезпечення, та шахрайство.

Женевські конвенції 1949 і Додаткові протоколи 1977 – ці документи прямо не згадують кіберпростір, але їх принципи міжнародного гуманітарного права застосовуються до всіх форм ведення війни, включно з кібервійною, але напряму не регулює кібервійни через свою застарілість [18].

Вони забороняють напади на цивільні об'єкти та вимагають від сторін конфлікту вживати всіх можливих заходів для запобігання випадкового пошкодження цивільних осіб та об'єктів.

В уставі ООН також не згадується кіберпростір, але його стаття 2 (пункт 4) забороняє використання сили проти територіальної цілісності або політичної незалежності будь-якої держави, а стаття 51 визнає право на самооборону в разі збройного нападу.

Таллінські посібники (1.0 та 2.0) ця література не є юридично обов'язковою, та вона представляє докладний аналіз застосування міжнародного права до кібероперацій в мирний час та під час збройних конфліктів. В ній надається інтерпретація існуючих норм щодо таких питань, як суверенітет, збройний напад, самооборона, та захист цивільних об'єктів у кіберпросторі.

З позитивних ініціатив можна зазначити паризький заклик за довіру та безпеку в кіберпросторі (2018) - ця ініціатива була запущена урядом Франції з метою зміцнення міжнародної безпеки та стабільності у кіберпросторі. Заклик був підтриманий багатьма державами та приватними організаціями та зосереджується на принципах відповідальної поведінки у кіберпросторі, не дивлячись на те, що він не є формальним міжнародним договором, такі ініціативи мають корисний вплив на підвищення рівню кіберзахищенності в світі.

На сьогоднішній день міжнародне регулювання кіберконфліктів залишається недостатньо розвинутим і часто не відповідає швидкому технологічному прогресу у цій сфері. Існуючі міжнародні угоди, такі як Будапештська конвенція про кіберзлочинність або Женевські конвенції, хоч і забезпечують загальні рамки для певних аспектів кібербезпеки, та вони не були спеціально розроблені для регулювання кібервійн або кібератак. Це створює суттєві прогалини в правовому регулюванні, особливо в контексті атрибуції та відповідальності за кібератаки. Незважаючи на існування деяких ініціатив, таких як Група урядових експертів ООН та Паризький заклик, суттєвий міжнародний діалог та розвиток специфічних міжнародних норм, які безпосередньо регулюють кіберконфлікти, все ще залишаються на

початковому етапі. Швидкий розвиток технологій, особливо у сфері кібербезпеки, ставить перед міжнародним співтовариством виклик адаптувати правові стандарти до цих нових реалій, що наразі відбувається недостатньо ефективно та оперативно.

Хоча конкретний міжнародний договір про кіберзброю ще не був укладений, існує загальне розуміння серед міжнародної спільноти щодо необхідності регулювання цього питання. Наразі обговорюються різні підходи, включаючи розширення існуючих договорів про зброю (наприклад, Конвенцію про заборону біологічної та токсичної зброї) для включення кіберзброї.

2.8 Психологічні аспекти кібервійни

Кібератаки мають значний вплив на різні верстви суспільства та окремих осіб. Це стосується не лише маніпуляції громадською думкою через розповсюдження дезінформації та пропаганди в інтернеті, але й викликає відчуття стресу та тривоги серед населення через потенційні загрози різного роду атак. Несподівані кібератаки можуть призвести до втрати важливих послуг або особистих даних, створюючи відчуття вразливості та безпорадності.

Військовослужбовці та спеціалісти з кібербезпеки також відчувають високий рівень стресу та психологічного тиску, пов'язаного з постійною загрозою як кібер, так і звичайних атак та необхідністю підтримувати цифрову безпеку та гігієну. Кібервійна використовується як інструмент психологічної війни для деморалізації населення або військових сил противника, розповсюджуючи неправдиву інформацію та створюючи паніку.

Для протистояння психологічним атакам важливо підвищувати обізнаність громадськості про кіберзагрози та розвивати освітні програми, що допомагають людям розуміти та адаптуватися до цих викликів. Підвищення рівня знань та обізнаності може допомогти зменшити тривогу та створити більш стійке суспільство. Крім того, необхідно звертати увагу на психологічну підтримку громадян, для запобігання професійного вигорання та інших психічних проблем. Осмислення психологічних аспектів є ключовими для ефективного управління кіберзагрозами та забезпечення національної безпеки.

2.8.1 Вплив кібервійн на громадську думку та психологію населення

Вплив кібератак на громадську думку та психологію населення . Ця сфера включає маніпуляцію інформацією, де кібероперації використовуються для розповсюдження дезінформації та пропаганди, здатні впливати на політичні погляди та виборчі процеси. Особливо це стає критичним, коли мова йде про міжнародні конфлікти, де фейкові новини та маніпулятивні повідомлення можуть значно викривляти реальність, створюючи помилкове уявлення про події чи осіб.

Поряд з цим, кібервійни впливають на психологію населення, викликаючи почуття небезпеки та невизначеності, особливо в разі атак на критичну інфраструктуру. Такі інциденти можуть призвести до втрати особистих даних або порушення приватності, збільшуючи рівень тривожності серед людей. Широкомасштабні кібератаки також можуть спричиняти стрес та паніку, особливо у районах, що знаходяться в зоні активних конфліктів.

Постійна військова кібердіяльність та використання кіберпростору для маніпулювання може мати довгострокові наслідки для психічного здоров'я

громадян, включаючи зростання випадків депресії та тривожних розладів. Це підкреслює важливість розробки стратегій кіберзахисту та психологічної підтримки населення, щоб мінімізувати негативний вплив кібератак на суспільство.

Ця сфера включає маніпуляцію інформацією, де кібероперації використовуються для розповсюдження дезінформації та пропаганди, здатні впливати, як на політичні погляди, так і на виборчі процеси. Особливо це стає критичним, коли мова йде про міжнародні конфлікти, де фейкові новини та маніпулятивні повідомлення можуть значно викривляти реальність, створюючи помилкове уявлення про події чи осіб.

2.9 Вплив кібервійни на критичну інфраструктуру

Кібератаки на критичну інфраструктуру України стали важливою частиною гібридної війни, яка розгорнулася в регіоні після вторгнення росії. Ці атаки включають різноманітні методи та стратегії, від DDOS (Distributed Denial of Service) атак до розширеного шпигунства і саботажу. Їх метою зазвичай є паралізувати основні функції держави, зокрема енергетичні системи, телекомунікації, банківську сферу, та інші життєво важливі сегменти.

Перша і найбільш помітна кібератака була здійснена в 2015 році на енергетичну систему України, що призвело до масштабного відключення електроенергії. Це була одна з перших відомих кібератак, яка безпосередньо спричинила фізичні збої в роботі критичної інфраструктури.

Перша значна кібератака на критичну інфраструктуру України, яка сталася 23 грудня 2015 року, була спрямована на енергетичний сектор країни. Цілью атаки були декілька обласних енергетичних компаній, що призвело до

масштабного відключення електроенергії. Зловмисники розпочали атаку з фішингової кампанії, яка дозволила їм отримати доступ до облікових записів працівників та подальшого контролю над системами управління та нагляду (SCADA) енергетичних компаній. Використання цього доступу дало можливість відключити електроенергію в різних регіонах України, внаслідок чого понад 230 тисяч людей залишилися без електрики на кілька годин Івано-Франківській області, що стало першим випадком, коли кібератака призвела до порушення роботи електромережі [19].

У ході атаки було використано спеціалізоване шкідливе програмне забезпечення, здатне впливати на промислові контрольні системи. Відновлення роботи систем вимагало переходу на ручне управління обладнанням. Ця подія стала серйозним викликом для України та підкреслила необхідність підвищення рівня кіберзахисту на національному та міжнародному рівнях. Атака привернула увагу міжнародної спільноти до проблем кібербезпеки, особливо у контексті захисту критичної інфраструктури, та спонукала уряди та приватний сектор по всьому світу посилити свої зусилля у цій сфері.

Для цієї атаки зловмисники використали шкідливе програмне забезпечення під назвою "BlackEnergy". "BlackEnergy" є високоспеціалізованим шкідливим ПЗ, яке первісно було розроблене як засіб для здійснення DDoS-атак (Distributed Denial of Service). Проте з часом його було значно модифіковано та адаптовано для різних цілей, включаючи кібершпіонаж та знищення даних. Під час атаки у 2015 році по енергетичним компаніям , BlackEnergy використовувався для злому та отримання доступу до систем управління енергетичними компаніями, а також для виконання дій, які призвели до відключення електроенергії.

Це ПЗ зазвичай поширюється через фішингові електронні листи з інфікованими вкладеннями. Після активації в системі, BlackEnergy може виконувати різноманітні завдання, включаючи крадіжку даних, знищення

файлів, а також втручання у роботу промислових контрольних систем. Це шкідливе ПЗ вважається досить складним і гнучким інструментом у руках кіберзлочинців [20].

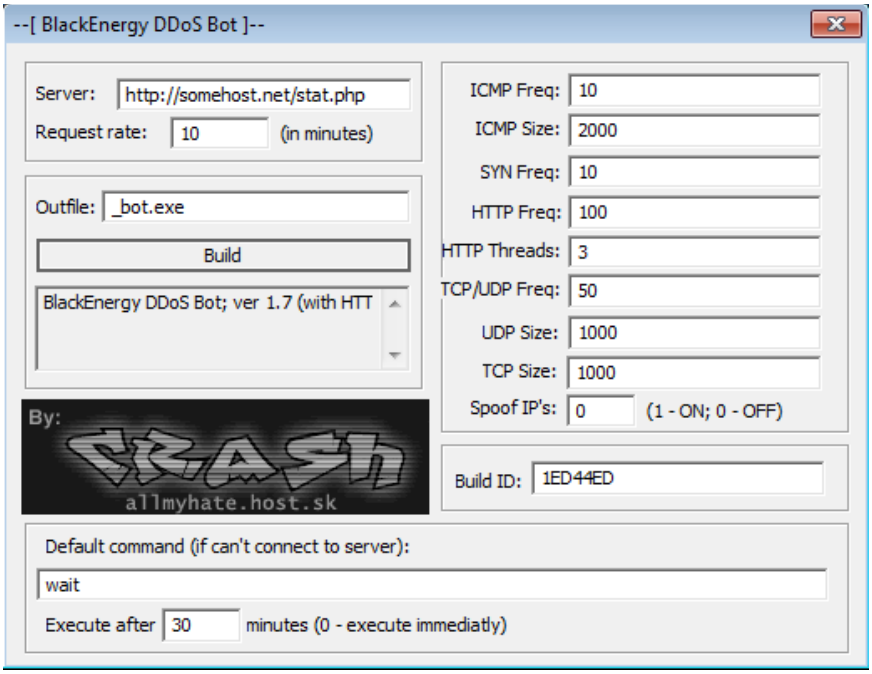

Рисунок 2.5 – Графічний інтерфейс ПЗ “BlackEnergy”

Його первісною метою було проникнення на веб-сайти російських фінансових установ, розповсюдження по їх мережах з метою вилучення фінансових даних для незаконного використання. Зауважимо, що програма була примітна своєю простотою, мала зручний графічний інтерфейс і навіть супроводжувалась простими інструкціями в стилі "для чайників".

У відповідь на це, Україна значно посилила свої кіберзахистові зусилля. Було вжито заходів для підвищення рівня захисту критичних систем, в тому числі через міжнародну співпрацю та обмін кіберрозвідданими, Україна налагодила тісну співпрацю з міжнародними партнерами у сфері кібербезпеки. Річ йде про обмін інформацією та даними розвідки, що дозволяє ефективніше протидіяти кіберзагрозам.. Крім того, Україна активно працює над

підготовкою кадрів у сфері кібербезпеки та розробкою власних кіберзахисних технологій, був зроблен ухил на підвищення кваліфікації та навчанні спеціалістів в галузі кібербезпеки, методом розвитку освітніх програм, а також тренінгів для підготовки та обміну досвідом висококваліфікованих фахівців, що були спроможні дати відсіч сучасним кіберзагрозам.

Однак, не дивлячись на ці заходи, кібератаки продовжують бути серйозною загрозою. Вони часто характеризуються високим рівнем складності та адаптивності, що вимагає постійного оновлення захисних стратегій. Це підкреслює важливість постійної уваги та інвестицій у кібербезпеку на національному рівні.

В цілому, ситуація з кібератаками на критичну інфраструктуру України вимагає комплексного підходу, що включає технічні, правові та стратегічні аспекти. Це стає ключовим елементом національної безпеки країни та її здатності протистояти гібридним загрозам.

2.9.1 Заходи захисту та відновлення після кібератак

Кібератаки стають все більш розповсюдженими та складними, створюючи значні виклики для організацій та індивідуумів. У цьому контексті, розуміння та впровадження ефективних заходів захисту та стратегій відновлення після кібератак є критично важливими для забезпечення безпеки інформації, а також збереження довіри та стабільності в цифровому просторі.

Ці заходи не тільки захищають від потенційних загроз, але й гарантують, що організації мають засоби для швидкого відновлення після інцидентів, мінімізуючи перерви в роботі та збитки. У цій статті ми розглянемо основні аспекти захисту та відновлення після кібератак, включаючи профілактичні

заходи, методи реагування на інциденти та стратегії запобігання майбутнім атакам.

Ці заходи можна умовно поділити на наступні кроки:

– запобіжні заходи;

– ідентифікація та реагування на атаки;

– відновлення після атаки;

– аналіз та покращення.

Починати треба з розробки запобіжних заходів. Важливо встановити сильні паролі та використовувати багаторівневу автентифікацію, регулярно оновлювати програмне забезпечення для усунення вразливостей, шифрувати дані, встановлювати та оновлювати антивірусне програмне забезпечення, а також проводити навчання персоналу про ризики та сучасні тактики кіберзлочинців.

У разі виявлення кібератаки, швидке реагування може значно зменшити збиток. В цьому контексті можна говорити про використання систем моніторингу для виявлення атаки, швидке ізолювання заражених систем для обмеження поширення та оцінку обсягу та впливу атаки.

Після цього, ключовим етапом є відновлення нормального функціонування, що включає використання резервних копій, що потрібні для відновлення втрачених даних, поступове відновлення послуг та функцій, а також внесення змін у системи безпеки для запобігання ймовірним повторним атакам.

Нарешті, після відновлення важливо провести глибокий аналіз інциденту, вивчити причини та методи атаки, внести відповідні зміни в політики та процедури безпеки, а також оновити програми навчання персоналу, враховуючи отриманий досвід. Це допомагає забезпечити більш міцний захист в майбутньому та підвищити загальну стійкість організації до кіберзагроз [20].

2.10 Висновки до розділу 2

В другому розділі робимо ухил на аналіз кібервійни в Україні, фокусуючись на зростанні кібератак, їх впливі та наслідках. Бачимо, що значно зросла кількість атак, особливо під час російсько-української війни. Мета в цих атак була різна, їх використовували з метою залякування, шпигунства та дестабілізації суспільства. Атаки були скеровані на урядові сайти, фінансові, енергетичні та оборонні системи.

Описано також й відповідь України, яка включає створення ІТ-армії для контратак в кіберпросторі. Підкреслюється важливість оновлення підходів до кібербезпеки, а також роль криптографії у захисті даних та систем.

В цілому, кібервійна являє собою значний компонент сучасних війн та конфліктів, вимагаючи суттєвої уваги зі сторони суспільства та держави до кібербезпеки та нормування в рамках кібербезпеки. Можна з легкістю прогнозувати, що у майбутньому кількість кібератак як й кількість збитків від них буде тільки рости, так що щоб зменшити ці збитки в перспективі, треба починати діяти прямо зараз.

3 СТВОРЕННЯ ТА АНАЛІЗ ПОТЕНЦІЙНОГО СЦЕНАРІЮ КІБЕРАТАК, РЕКОМЕНДАЦІЇ ЩОДО ЗАКОНОДАВСТВА ТА ПРОТИДІЇ КІБЕРАТАКАМ

3.1 Вибір об’єкта для кібератак

Для цього аналізу була обране державне акціонерне товариство залізничного транспорту загального користування “Укрзалізниця”. Вона була обрана виходячи з того, що залізничний транспорт є життєво важливим для економічної стабільності та ефективності логістичних ланцюгів. Він забезпечує перевезення великих обсягів товарів та пасажирів по всій країні. Перебої в роботі залізниці можуть мати серйозні наслідки для економіки, впливаючи на торгівлю, промисловість та сільське господарство.

Немалу роль вона відіграє й у воєнних та гуманітарних операціях. У контексті війни в Україні, залізничний транспорт часто використовується для переміщення військової техніки, боєприпасів та військовослужбовців. Також він має важливе значення для гуманітарних операцій, забезпечуючи доставку необхідних ресурсів у райони, що постраждали від військових дій та забезпечує евакуаційні коридори для цивільного населення .

Крім цього велике значення під час війни мають об’єкти-символи. Залізнична система ж є символом національної єдності та стабільності. Її зрив може послабити моральний дух населення і підірвати віру в ефективність уряду та військових структур.

3.1.1 Сруктура та характеристика “Укрзалізниці”

"Укрзалізниця" (УЗ) представляє собою державну залізничну компанію України, яка є однією з найбільших у Європі за розміром мережі та обсягом перевезень. Компанія виконує важливу роль у національній економіці, забезпечуючи пасажирські та вантажні залізничні перевезення. Вона охоплює широкий спектр діяльності, включаючи обслуговування міського електричного транспорту, міжміських та міжнародних поїздів, а також займається логістикою та управлінням вантажними перевезеннями.

Щодо інфраструктури, Укрзалізниця управляє значною кількістю залізничних станцій, сигналізаційними системами, мостами та іншими об'єктами, які необхідні для забезпечення безперебійної та безпечної роботи залізничного транспорту. Компанія також приділяє значну увагу модернізації та впровадженню новітніх технологій для поліпшення якості своїх послуг та підвищення безпеки руху.

Управлінська структура Укрзалізниці включає верхівку, призначену урядом, та різні управлінські рівні. Компанія часто поділяється на регіональні філії для ефективнішого управління та експлуатації залізничних мереж у різних частинах країни. До структури також входять логістичні та технічні відділи, які відповідають за планування та управління транспортними потоками, технічне обслуговування та інші важливі аспекти діяльності. Окрім того, є фінансові та адміністративні відділи, які займаються бухгалтерським обліком, кадровими питаннями та іншими адміністративними функціями.

Загалом, Укрзалізниця відіграє ключову роль у забезпеченні транспортних послуг в Україні, гарантуючи мобільність громадян та перевезення товарів, що є важливим для економічного розвитку та зв'язку між різними регіонами країни.

3.1.2 Сценарій кібератаки

Розглянемо сценарій модельованої кібератаки на "Укразалізницю". Мета такого сценарію - наголосити на важливості кібербезпеки та можливих методах захисту. Розробити ефективні методи протидії можливим кібератакам й навести дієві методи боротьбі з можливими ураженнями.

Як приклад візьмемо фішингову атаку, з метою встановлення шкідливого ПЗ.

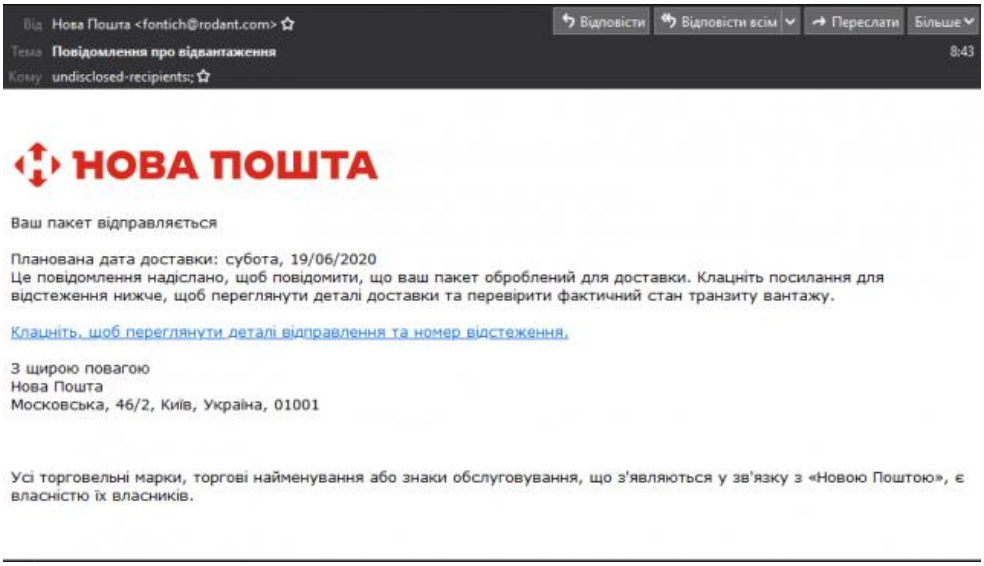

Рисунок 3.1 – Приклад фішингового листа від компанії “Нова пошта” [22]

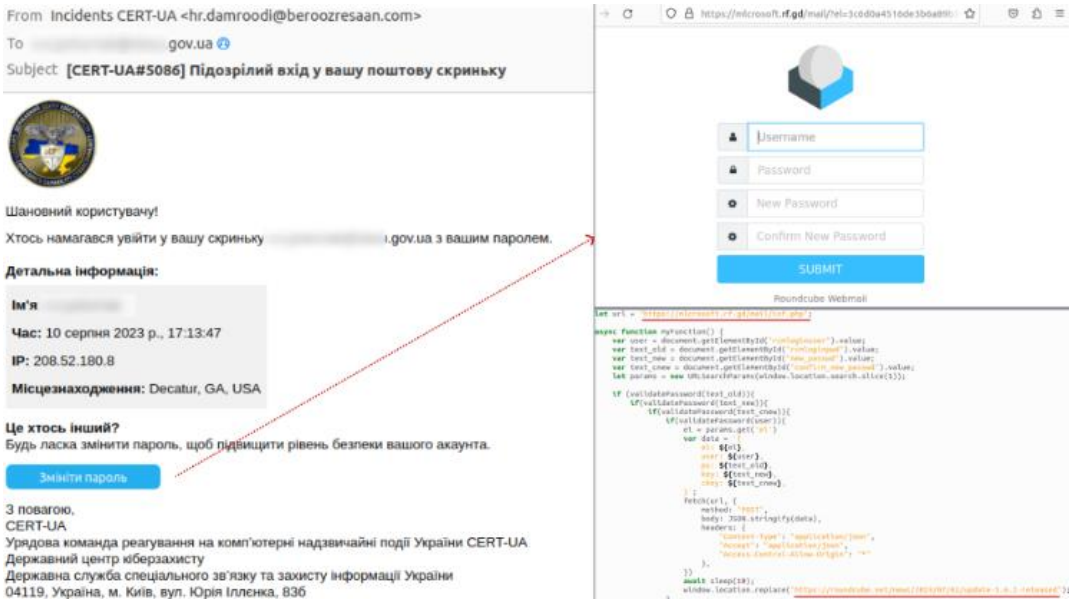

Рисунок 3.2 – Фішингові електронні листи з символікою Держспецзв'язку [23]

Під час фішингової атаки, зловмисники будуть ставити собі на меті маскування під довірених осіб або організації з метою отримання конфіденційної інформації, такої як логіни та паролі, даних про внутрішню інфраструктуру, доступ до корпоративних електронних пошт, комерційних даних, особистих даних співробітників, доступу до систем управлінь та до інформації про клієнтів:

– логіни та паролі: однією з основних цілей фішингу є отримання логінів та паролів співробітників, що дає доступ до внутрішніх систем компанії.

– доступ до корпоративних електронних пошт: зловмисники можуть використовувати доступ до корпоративних поштових акаунтів для подальших фішингових атак або для розсилки шкідливих програм.

– дані про внутрішню інфраструктуру: інформація про мережеву інфраструктуру, сервери, використовуване програмне забезпечення тощо може бути використана для планування подальших кібератак.

– конфіденційні комерційні дані: інформація про контракти, фінансові операції, стратегічні плани компанії.

– особисті вані співробітників: інформація про співробітників, така як ідентифікаційні номери, адреси, банківські реквізити тощо, може бути використана для шахрайства або ідентифікаційного крадіжки.

– доступ до систем управління рухом: в разі залізничної компанії, отримання доступу до систем управління рухом поїздів може мати серйозні наслідки для безпеки.

– інформація про клієнтів: дані про пасажирів, такі як контактні дані, інформація про бронювання тощо.

Ціль фішингової атаки в такому випадку не тільки в крадіжці інформації, але й у здатності використовувати цю інформацію для подальшого проникнення в системи компанії, її маніпуляції та потенційного завдання шкоди.

Наступним кроком стане встановлення шкідливого ПЗ. Коли співробітник компанії відкриває таке вкладення або переходить за таким посиланням, шкідливе програмне забезпечення автоматично встановлюється на його комп'ютері, часто без будь-яких зовнішніх ознак або попереджень.

Шкідливе ПЗ, щойно активоване, може виконувати різноманітні дії відповідно до свого програмування і цілей зловмисника. Наприклад, воно може викрадати конфіденційні дані, здійснювати моніторинг діяльності користувачів, поширюватися по мережі для інфікування інших систем, або навіть блокувати доступ до важливих файлів або систем. Часто виявлення такого ПЗ відбувається тільки після того, як воно завдає шкоди або протягом тривалого часу незамітно збирає інформацію.

Прикладів такого шкідливого програмного забезпечення існує багато, усі вони використовують різноманітні вразливості та мають власні цілі після попадання у мережу:

– WannaCry: це відомий рансомвар, який шифрує файли на заражених комп'ютерах, вимагаючи викуп за їх розшифровку. WannaCry поширювався по всьому світу в 2017 році, використовуючи вразливість у Windows для автоматичного поширення по мережах;

– Petya/NotPetya: ще один приклад рансомвару, який блокує доступ до комп'ютерів і вимагає викуп. NotPetya особливо відомий своїми атаками на українські компанії у 2017 році;

– Emotet: первісно відомий як банківський троян, Emotet еволюціонував у потужну мережу для розповсюдження інших видів шкідливого ПЗ. Він може використовуватися для встановлення воріт для інших типів шкідливих програм на заражених комп'ютерах;

– Mirai: ботнет використовує вразливі IoT пристрої для створення величезної мережі заражених пристроїв, які можуть бути використані для DDoS-атак;

– Stuxnet: хоча він вже застарів, Stuxnet був одним із перших шкідливих програм, розроблених для конкретної мети - пошкодження іранських ядерних об'єктів. Це був складний вірус, який міг поширюватися через мережі без Інтернету;

– Trickbot: це банківський троян, який використовує модульну структуру для крадіжки банківських даних і поширення інших видів шкідливого ПЗ;

– Ryuk: рансомвар, який вибірково атакує свої цілі та був відповідальний за ряд значних атак на організації по всьому світу.

Частина з цього шкідливого ПЗ вже використовувалось для атак по Україні в минулому, а саме:

– Petya/NotPetya: цей рансомвар став особливо відомий через свої атаки на українські компанії у червні 2017 року. NotPetya швидко поширився з України на міжнародний рівень, завдавши значних збитків компаніям по

всьому світу. Він використовував вразливості в Microsoft Windows для поширення всередині корпоративних мереж;

– WannaCry: він не був специфічно спрямований на Україну, цей рансомвар мав глобальний вплив і також зачепив системи в Україні під час свого масового поширення у 2017 році;

– BlackEnergy: це шкідливе ПЗ було використане для кібератак на українські енергетичні об'єкти в кінці 2015 року, що призвело до значних відключень електроенергії. Атаки з BlackEnergy були складно організовані та включали використання троянських програм і компонентів для знищення даних.

Наступним кроком стане отримання контролю над мережою. Це може надати зловмисникам доступ до критично важливих систем і інформації. Наведемо деякі приклади потенційних цілей такої атаки:

– системи управління рухом поїздів: контроль над цими системами може дозволити зловмисникам маніпулювати розкладами, маршрутами, а також сигналізацією, що може мати серйозні наслідки для безпеки руху;

– логістична інформація: доступ до логістичних систем дозволить зловмисникам дізнатися про маршрути, графіки та вантажі, що перевозяться, включаючи військові та гуманітарні вантажі;

– комунікаційні системи: зловмисники можуть перехоплювати або блокувати комунікації всередині компанії, ускладнюючи координацію та управління;

– бази даних із особистою інформацією: доступ до особистої інформації співробітників та пасажирів може бути використаний для ідентифікаційного крадіжки або шантажу;

– фінансові системи: атаки можуть бути спрямовані на фінансові відділи компанії, що може призвести до витоку фінансової інформації, крадіжки коштів або шкоди фінансовій стабільності компанії;

– інфраструктурні системи: це може включати контроль над системами управління енергопостачанням, освітленням, водопостачанням тощо, що критично важливо для функціонування залізничних станцій та іншої інфраструктури.

3.1.3 Наслідки від цієї атаки

Кібератака на компанію, що займається залізничним транспортом в Україні, може мати різноманітні та серйозні наслідки, особливо в умовах війни. Перш за все, це може викликати значні перебої в залізничних перевезеннях, включаючи як пасажирські, так і вантажні перевезення. Такі перебої не тільки спричинять незручності для пасажирів, але й можуть мати серйозні економічні наслідки, порушуючи логістику та поставки важливих товарів та ресурсів, включаючи гуманітарні вантажі. Враховуючи критичну роль залізниці в українській економіці, особливо у промисловому та аграрному секторах, такі перебої можуть завдати серйозної шкоди економічному зростанню країни.

На військовому фронті, залізниця часто використовується для перевезення військових вантажів та особового складу, тому атака на залізничну систему може мати негативні наслідки для обороноздатності країни. Перешкоди в перевезенні військового обладнання та ресурсів можуть ослабити військові операції та вплинути на загальний стан безпеки в країні. Крім того, залізниця є важливою для евакуації цивільного населення з зон конфлікту, тому її зупинка або порушення може мати серйозні гуманітарні наслідки.

Кібератака також може призвести до витоку конфіденційної інформації, що становить загрозу не тільки для компанії, але й для національної безпеки.

Така інформація може включати деталі військових перевезень, розклади та маршрути, а також особисті дані співробітників та пасажирів. В умовах війни, це може бути використано ворожими силами для планування атак або саботажу.

Моральний та психологічний вплив також не можна недооцінювати. У ситуації, коли населення вже переживає стрес через військовий конфлікт, додаткові загрози, такі як кібератаки, можуть збільшити відчуття тривоги та невизначеності. Це може вплинути на загальний моральний дух населення та посилити соціальну нестабільність.

Таким чином, кібератака на залізничну інфраструктуру в умовах війни може мати далекосяжні наслідки, що впливають на безпеку, економіку, військові операції та соціальний стан країни.

3.1.4 Протидія кібератакам

Ефективна протидія таким атакам вимагає всебічного підходу, що поєднує в собі технологічні, організаційні та освітні стратегії. Важливо не тільки застосовувати передові технічні рішення для захисту мереж та систем, але й забезпечувати постійне навчання співробітників, розробку ефективних процедур реагування на інциденти та активне співробітництво з органами безпеки та експертами з кібербезпеки. Усвідомлення потенційних загроз та їх впливу на критичні аспекти діяльності компанії є ключовим для розробки та впровадження ефективних заходів протидії.

Детально оглянемо можливі заходи, розпочнемо з технічних заходів:

– зміцнення безпеки мережі: важливо забезпечити мережу міцними брандмауерами та іншими системами виявлення та запобігання вторгненням.

Також корисно впровадження розширеного моніторингу мережі для виявлення підозрілої активності;

– регулярні оновлення та патчі необхідні всі системи та програмне забезпечення повинні регулярно оновлюватися для усунення вразливостей, які можуть бути використані в кібератаках;

– шифрування даних є важливою складовою в захисті інформації, важливо забезпечити шифрування конфіденційної інформації, особливо тієї, що передається через мережу;

– сегментація мережі є дієвим елементом захисту інформації, по аналогії з залізничним составом, розділення мережі на сегменти може запобігти поширенню шкідливого програмного забезпечення в разі його проникнення;

– резервне копіювання та відновлення: регулярне створення резервних копій критично важливих даних та систем є ключовим для швидкого відновлення після атаки.

Далі розглянемо не менш важливі заходити треба не забувати уділяти їм велике значення, мова йде про організаційні заходи, до них можна віднести:

– політика безпеки та навчання персоналу, а саме розробка та впровадження чіткої політики кібербезпеки, а також регулярне навчання співробітників, є ключовими для зміцнення загальної безпеки;

– розробка плану реагування на інциденти, компанія повинна мати детальний план реагування на кібератаки, включаючи процедури виявлення, ізоляції атаки та відновлення систем;

– аудит та тестування безпеки є необхідною опцією, регулярний аудит та тестування систем на вразливості є необхідними для виявлення потенційних слабких місць;

– співпраця з органами безпеки: співпраця з національними та міжнародними органами безпеки може допомогти в обміні інформацією про загрози та найкращі практики в області кібербезпеки;

– правова підготовка: розуміння та дотримання відповідних законів та регуляцій з кібербезпеки також є важливим.

Важливим аспектом покращення захищеності вашої системи є співпраця с експертами з кібербезпеки. Налагодження партнерства з експертними організаціями в сфері кібербезпеки може надати додаткові ресурси, знання та підтримку для зміцнення оборонних засобів компанії. За можливістю правильним буде створення відділу з кібербезпеки, або наймати окремих спеціалістів з галузі кібербезпеки [24].

Протидія кібератакам вимагає багатовимірного підходу, що поєднує технологічні інновації з організаційними стратегіями та постійним навчанням. В умовах війни та політичної нестабільності, такий підхід стає ще більш критичним для забезпечення надійної захисту ключових об’єктів інфраструктури.

3.2 Рекомендації щодо протидії кібератакам

Особливе становище України як країни, що переживає геополітичні напруження та війну, вимагають конкретних рекомендацій щодо протидії кібератакам.

Забезпечення розвитку кібербезпекової індустрії в Україні, включаючи розробку та виробництво кібербезпекових технологій, інструментів та рішень. Створення національних компетенційних центрів з кібербезпеки та сприяння партнерству між державними органами, академічними установами та приватним сектором.

Звернення особливої уваги на захист критичної інфраструктури, такої як енергетика, транспорт, медичні системи тощо, від кібератак. Розробка стратегічних планів кіберзахисту, впровадження стандартів та виявлення вразливостей в цих сферах.

Залучення до міжнародних спільних проектів, обмін досвідом та інформацією з іншими країнами. Участь в міжнародних ініціативах щодо кібербезпеки, таких як програми навчання, спільні практики та обмін інформацією про загрози та інциденти. Наразі на стороні України у кіберпросторі воюють тисячі людей зі всього світу, серед яких є організації та проекти з гучними іменами, які зарекомендували себе як досвідчені спеціалісти, треба розробити програму по співпраці з ними на постійній основі та урегулювати її дії.

Продовження розвитку освітніх програм та свідомості про кібербезпеку в Україні. Особлива увага має бути приділена підвищенню обізнаності серед державних службовців, бізнесу та громадян щодо ризиків кібератак та заходів захисту.

Стимулювання наукових досліджень та розробок у галузі кібербезпеки. Сприяння створенню інноваційних стартапів та компаній, що працюють у сфері кібербезпеки, та підтримка розвитку кібербезпечних технологій в Україні.

Необхідно забезпечити ефективного партнерства між державним сектором, приватними компаніями, громадськістю та академічними установами. Спільна розробка та впровадження стратегій з кібербезпеки, обмін інформацією та координація дій у випадку кібератак.

Та окрім цього не треба забувати про особисту цифрову гігієну, вмикаючи комп’ютер, або заходячи у браузер телефону, ви можите стати мішенями окупантів, а тому піклування про власну кібербезпеку є вкрай важливим. Ніколи не натискати на невідомі посилання, ніколи не вводьте свої особисті дані на будь яких ресурсах, у надійності яких ви не впевнені. Перед

тим, як поширювати інформацію про себе чи про свої банківські картки, запитайте себе: "Що це за сайт? Звідки я дізнався про нього? Чи довіряю я людині, яка дала мені це посилання?". Якщо ви не впевнені, перепитайте у інших людей, чи вони знають такий ресурс". Використовуйте надійні паролі, користуйтеся надійними антівірусами. Встановлюйте лише ліцензіонні програми лише з офіційних джерел та робіть бекапи, резервні копіювання даних [25].

Можна виділити наступні технічні заходи для забезпечення кібербезпеки:

– IDPS;
– Криптографічний захист даних;
– Оновлення та патчі;
– Фаєрволи та антивірусне ПЗ;
– Багатофакторна аутентифікація;
– Резервне копіювання.

IDPS (системи виявлення та запобігання вторгнень) є комплексними системами, які виконують не тільки функцію виявлення ознак вторгнення чи шкідливої діяльності у мережі чи системах, але й активно запобігають цим вторгненням. Вони працюють шляхом моніторингу мережевого трафіку та системної активності на предмет відхилень від норми. При виявленні підозрілих дій система може автоматично вжити заходів, таких як блокування трафіку або відключення підозрілих процесів.

Криптографічний захист даних застосовує шифрування для забезпечення конфіденційності та цілісності інформації. Цей процес включає шифрування даних з використанням спеціального ключа перед їх зберіганням або передачею, а також використання відповідного ключа для дешифрування, щоб отримати доступ до цих даних.

Оновлення та патчі є важливою частиною утримання програмного забезпечення в актуальному стані. Вони випускаються розробниками для

виправлення помилок, усунення вразливостей та внесення поліпшень. Ці оновлення можуть автоматично встановлюватися або вимагати ручного втручання і є ключовими для захисту від відомих загроз.

Фаєрволи та антивірусне програмне забезпечення служать для захисту комп'ютерних систем від вірусів, шпигунських програм та інших мережевих атак. Фаєрволи контролюють вхідний та вихідний трафік, блокуючи або дозволяючи певні з'єднання згідно з встановленими правилами, тоді як антивірусне ПЗ сканує системи для виявлення та усунення шкідливих програм.

Багатофакторна аутентифікація (MFA) забезпечує додатковий рівень безпеки, використовуючи два або більше незалежних критеріїв: щось, що користувач знає (наприклад, пароль), щось, що він має (таке як токен або смартфон), або щось, що він є (наприклад, біометричні дані). Це значно ускладнює несанкціонований доступ.

Резервне копіювання є процесом створення копій важливих даних для запобігання їх втраті у разі поломок обладнання, кібератак чи інших непередбачених обставин. Дані регулярно копіюються на окремі носії, такі як зовнішні диски, хмарні сервіси або віддалені сервери, забезпечуючи можливість їх відновлення у разі потреби.

3.3 Пропозиції щодо розвитку українського законодавства

Подальший розвиток українського законодавства у сфері кібербезпеки та кібервійни має включати в себе декілька ключових напрямків. Перш за все, потрібно активізувати процес перегляду та оновлення існуючого законодавства в контексті швидкого розвитку цифрових технологій.

Водночас, особливої уваги вимагає створення ефективного механізму реагування на кібератаки, що має включати в себе не тільки технічні, але й організаційні, правові та міжнародні аспекти. Відповідне законодавство має визначати як функції та обов'язки різних державних структур у випадку кібератаки, так і механізми координації дій з міжнародними партнерами.

Не менш важливою є підготовка кваліфікованих спеціалістів у сфері кібербезпеки. Держава має стимулювати розвиток відповідних освітніх програм та курсів, а також встановлювати вимоги до кваліфікації спеціалістів, які займаються захистом від кібератак.

Важливим є також питання захисту критичної інфраструктури від кібератак. Законодавство має визначати механізми захисту критичної інфраструктури, розробляти стандарти безпеки, проводити регулярні аудити та встановлювати штрафи за недотримання норм безпеки.

Також, необхідно забезпечити законодавчу підтримку інформаційних кампаній, спрямованих на підвищення обізнаності громадян про загрози кібербезпеки та способи їх запобігання. Зокрема, потрібно створити механізми, які б допомагали громадянам зрозуміти, як вони можуть захистити себе від кібератак і шахрайства в інтернеті [26].

3.4 Висновки до розділу 3

Цей розділ дипломної роботи розглядає створення та аналіз потенційних сценаріїв кібератаки на "Укрзалізницю" із рекомендаціями щодо законодавства та контрзаходів. Він висвітлює важливість кібербезпеки для такої критичної інфраструктури. Презентовано гіпотетичний сценарій кібератаки, що включає фішинг та встановлення шкідливого ПЗ, та обговорюються його потенційні наслідки.

ВИСНОВКИ

Кібервійна є серйозною загрозою для безпеки, економічного розвитку, політичної стабільності та приватності в сучасному світі. Україна, як і багато інших країн, стикається зі значними викликами у галузі кібербезпеки та кібервійни. Кібератаки спрямовуються на різні сектори, включаючи енергетику, транспорт, фінансові установи та інші, і можуть мати серйозні наслідки.

Протидія кібервійні вимагає комплексного підходу та співробітництва між державою, приватним сектором та громадськістю. Важливо підвищити свідомість та освіту про кібербезпеку, розвивати кібербезпекову інфраструктуру, зміцнювати законодавство та сприяти міжнародному співробітництву. Крім того, необхідно забезпечити підвищення готовності, постійне оновлення технологій та розробку стратегічних планів кібербезпеки.

Україна повинна звернути особливу увагу на своє положення в контексті кібервійни. Треба застосувати конкретні рекомендації щодо розвитку кібербезпеки, зміцнення кібербезпекових заходів, підвищення свідомості та освіти, сприяння міжнародному співробітництву та удосконалення законодавства можуть допомогти забезпечити ефективну протидію кібервійні та забезпечити стійкість та безпеку в кіберпросторі.

Тільки через спільні зусилля всіх зацікавлених сторін можна досягти успіху у протидії кібервійні та створити надійне та безпечне кіберсередовище. Україна має використовувати всі наявні ресурси, створювати нові технології та партнерства для забезпечення кібербезпеки та захисту своїх інтересів у кіберпросторі.

Необхідним фактором є підвищення рівня обізнаності серед населення щодо інформаційної гігієни та проводити планомірну боротьбу з пропагандою, підтримуючи населення в протидії ворожим ІПСО. Своєчасне

надання інформації значно понижує рівень стресу та розповсюдження дезінформації у масах. Більша частина витоків інформації на даний момент коється через людський фактор, через недостатню обізнаність людей в сфері кібербезпеки.

Важливо розуміти, що зараз від військових дій у кіберпросторі залежать людськи життя, тому ми не можемо нехтувати ворожим кібератаками та повинні не тільки давати їм відсіч, але й наносити атаки у відповідь. Незважаючи на усі наші успіхи та досягнення на фронті, треба розуміти, що навіть після того, як усі окупанти покинуть території незалежної України, навіть після Дня Перемоги проти російського агресора, що звісно настане, ворог буде продовжувати проводити кібератаки проти України, та буде атакувати державу та громадян й надалі, саме тому важливо покращувати наші методи протидії цим атакам й надалі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. IBM 2022 Report: Cost of a Data Breach at an All-Time High. Cyware Social. URL: https://cyware.com/news/ibm-2022-report-cost-of-a-data-breach-at-an-all-time-high-9303d2b3 (дата звернення: 5.08.2023).

2. Що таке ІПСО (інформаційно-психологічні операції): форми і методи – Україна кримінальна. Україна кримінальна.
URL: https://cripo.com.ua/likbez/shho-take-ipso-informatsijno-psihologichni-operatsiyi-formi-i-metodi/ (дата звернення: 12.08.2023).

3. Історична правда. Американський агітпроп часів Другої світової (плакати). Частина 1. Історична правда.
URL: https://www.istpravda.com.ua/artefacts/4d38eea11b77d/ (дата звернення: 12.08.2023).

4. A group of young German boys view "Der Stuermer", "Die Woche," and other propaganda posters that are posted on a fence in Berlin. United States Holocaust Memorial Museum. URL: https://collections.ushmm.org/search/catalog/pa1154416 (дата звернення: 13.08.2023).

5. Contributors to Cyber SecTech Wiki. NotPetya Attack. Cyber SecTech Wiki. URL: https://cyber-sectech.fandom.com/wiki/NotPetya_Attack (дата звернення: 15.08.2023).

6. DDoS Threat Landscape - Russia | NETSCOUT. NETSCOUT. URL: https://www.netscout.com/blog/asert/ddos-threat-landscape-russia (дата звернення: 21.08.2023).

7. Українська правда. Хакери взломали сайти російських відомств. Українська правда.
URL: https://www.pravda.com.ua/rus/news/2022/03/8/7329537/ (дата звернення: 20.08.2023).

8. Як відбувається перша світова кібервійна. АрміяInform – Інформаційне агентство АрміяInform. URL: https://armyinform.com.ua/2023/02/01/yak-vidbuvayetsya-persha-svitova-kibervijna/ (дата звернення: 03.10.2023).

9. What Is Cryptography and Why Is It Important? - Entrust Blog. Entrust Blog. URL: https://www.entrust.com/blog/2021/06/why-is-cryptography-so-important-heres-what-you-need-to-know/ (дата звернення: 04.10.2023).

10. Cobb M. What is Triple DES and why is it being disallowed? | TechTarget. TechTarget. URL: https://www.techtarget.com/searchsecurity/tip/Expert-advice-Encryption-101-Triple-DES-explained (дата звернення: 06.10.2023).

11. Academic: The Twofish Encryption Algorithm - Schneier on Security. Schneier on Security. URL: https://www.schneier.com/academic/archives/1998/12/the_twofish_encrypti.html (дата звернення: 06.10.2023).

12. Advanced Encryption Standard (AES) - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/ (дата звернення: 10.10.2023).

13. Whatis RSA? How does an RSA work? | Encryption Consulting. Encryption Consulting. URL: https://www.encryptionconsulting.com/education-center/what-is-rsa/ (дата звернення: 14.10.2023).

14. What are the applications of cryptography in information security?. Tutorialspoint. URL: https://www.tutorialspoint.com/what-are-the-applications of cryptography in information security (дата звернення: 17.10.2023)

15. Supruniuk I. Yegor Aushev, CyberUnit.Tech & Cyber School: "Our mission is to elevate the perception of Ukraine as a country of innovation" · TechUkraine. TechUkraine. URL: https://techukraine.org/2022/06/30/yegor-aushev-cyberunit-tech/ (дата звернення: 01.12.2023).

16. Ukrinform. Кібербезпека в Україні: шляхи розвитку та можливості. Укрінформ. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення: 20.10.2023).

17. Статут ООН : Статут від 26.06.1945 р. : станом на 24 верес. 1973 р. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf (дата звернення: 20.10.2023).

18. На варті гуманності. Женевські конвенції 1949 - Юридична Газета. Юридична газета. URL: https://yur-gazeta.com/dumka-eksperta/na-varti-gumannosti-zhenevski-konvenciyi-1949.html (дата звернення: 30.10.2023).

19. Історія довжиною у 8 років: Україна як поле кібератак групи хакерів Sandworm. ESET. URL: https://www.eset.com/ua/about/newsroom/press-releases/malware/istoriya-dlinoy-v-8-let-ukraina-kak-pole-kiberatak-gruppy-khakerov-sandworm/ (дата звернення: 01.11.2023).

20. BlackEnergy Version 2 Threat Analysis. Secureworks. URL: https://www.secureworks.com/research/blackenergy2 (дата звернення: 02.11.2023).

21. 11 кроків на шляху до відновлення після фішингової атаки: рекомендації від lepide. Intelligent IT Distribution. URL: https://iitd.com.ua/news/11-krokiv-do-vidnovlennja-pislja-fishingovoi-ataki-rekomendacii-vid-lepide/ (дата звернення: 02.11.2023).

22. Хакери розсилають фішингові листи, маскуючи їх під листи від Нової пошти. GECID.com - огляди і новини світу IT. URL: https://ua.gecid.com/news/hakery_rassylayut_fishingovye_pisma/ (дата звернення: 04.11.2023).

23. "Змініть пароль до Roundcube": чергова фішингова атака з використанням атрибутів CERT-UA та символіки ДЦКЗ Держспецзв'язку (CERT-UA#7223). cert.gov.ua. URL: https://cert.gov.ua/article/5455833 (дата звернення: 08.12.2023).

24. Захист від ddos-атак. Intelligent IT Distribution. URL: https://iitd.com.ua/zashchita-ot-ddos-atak/ (дата звернення: 13.11.2023).

25. Рекомендації Держспецзв’язку щодо запобігання та протидії кібератакам. gov.ua. URL: https://www.kmu.gov.ua/news/250099405 (дата звернення: 09.11.2023).

26. Офіційний портал Верховної Ради України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657 (дата звернення: 10.11.2023).