Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«17» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Захист інформаційного сектору держави від кібервпливу під час кібервійни»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Вікторія ШМАТКО**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Микола БРАІЛОВСЬКИЙ	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Шматко Вікторії Олександрівні**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Захист інформаційного сектору держави від кібервпливу під час кібервійни

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Законодавство України, людський фактор при роботі SCADA, реалізовані техніки кібервпливу у 2022 році, заходи влади України проти кібервпливу на національному та міжнародному рівнях

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідність захисту критичної інфраструктури в умовах кібервійни, передумови передумови розгортання кібервійни в українському віртуальному просторі, заходи влади щодо захисту інформаційного сектору, розробка комплексу заходів захисту Від кібервпливу на персонал критично важливих об'єктів інфраструктури

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Реалізація універсального для будь-якої країни комплексу заходів щодо захисту її інформаційного сектору від кібервпливу під час кібервійни

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 р.

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ініціали, прізвище)
Завдання прийняв до виконання _____ Вікторія ШМАТКО
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки завдань	29.10.2021 – 26.01.2022	*виконано*
2	Аналіз джерел інформації	27.01.2022 – 06.02.2022	*виконано*
3	Розгляд проблеми захисту критичної інфраструктури під час кібервійни	07.02.2022 – 01.03.2022	*виконано*
4	Історія та значення кібервійни	02.03.2022 – 20.03.2022	*виконано*
5	Кібератаки на українські ресурси	21.03.2022 – 04.04.2022	*виконано*
6	Інформаційний сектор – сфера впливу Міністерства цифрової трансформації	05.04.2022 – 12.04.2022	*виконано*
7	Реєстр критичної інфраструктури інформаційного сектору	13.04.2022 – 25.04.2022	*виконано*
8	Ідентифікація та аналіз використаних технік кібервпливу	26.04.2022 – 11.05.2022	*виконано*
9	Розробка комплексу заходів щодо захисту від кібервпливу	12.05.2022 – 29.05.2022	*виконано*
10	Оформлення пояснювальної записки	30.05.2022 – 05.06.2022	*виконано*
11	Підготовка до захисту	06.06.2022 –14.06.2022	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ініціали, прізвище)
Завдання прийняв до виконання _____ Вікторія ШМАТКО
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, чотирьох розділів, висновків і списку використаних джерел. Основний текст займає 79 сторінок, включає в себе зміст, вступ, чотири розділи дипломної роботи, висновки та список джерел. Крім того, робота містить 1 додаток обсягом 1 сторінка. У пояснювальній записці дипломної роботи міститься 27 рисунків.

Метою роботи є провести дослідження небезпечного кібервпливу на суспільство (державу) під час гібридної війни та розробити відповідний захист інформаційного сектору держави.

Для досягнення зазначеної мети поставлено наступні *завдання*:

- розкрити необхідність захисту критичної інфраструктури в умовах кібервійни;
- простежити глобальні та локальні події, які стали передумовами кібервійни в українському віртуальному просторі;
- виконати аналіз заходів влади щодо забезпечення захисту інформаційного сектору;
- розробити комплекс заходів захисту від кібервпливу на персонал критично важливих об’єктів інфраструктури на основі такого, що відбувався протягом російського вторгнення на територію України з лютого по травень у 2022 році.

Об’єктом дослідження є процес здійснення кібервпливу на працівників критично важливих об’єктів інфраструктури інформаційного сектору.

Предметом дослідження є сукупність заходів для протидії кібервпливу на працівників критично важливих об’єктів інфраструктури інформаційного сектору.

Методи дослідження: системний аналіз, історичний метод, ізолювання, узагальнення, абстрагування.

Актуальність обраної теми дипломної роботи є безперечною, враховуючи розв’язану Російською Федерацією повноцінну гібридну війну та відсутність цілісного, конкретного та всебічного регулювання джерел інформації під час

кібервійни як частини гібридної війни, які становлять негативний вплив на персонал критично важливих об’єктів інфраструктури країни-жертви.

Практичною цінністю отриманих результатів є реалізація універсального для будь-якої країни мінімально необхідного комплексу заходів щодо захисту інформаційного сектору держави від кібервпливу під час кібервійни.

Ключові слова: кібервійна, критична інфраструктура, SCADA, кібервплив, персонал, пропаганда, дезінформація.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

CPR	–	Check Point Research.
HMI	–	Human Machine Interfaces.
IaaS	–	Infrastructure as a Service.
RTU	–	Remote terminal units.
SCADA	–	Supervisory Control and Data Acquisition.
ВСД	–	вищі структури держави.
Держспецзв’язку	–	Державна служба спеціального зв’язку та захисту інформації України.
ЗМІ	–	засоби масової інформації.
КВОІ	–	критично важливі об’єкти інфраструктури.
КІ	–	критична інфраструктура.
КСЗІ	–	комплексна системи захисту інформації.
Мінцифри	–	Міністерство цифрової трансформації України.
ОВСП	–	орган, відповідальний за спростування пропаганди.
ОКІІ	–	об’єкти критичної інформаційної інфраструктури.
Перелік	–	перелік секторів (підсекторів), основних послуг критичної інфраструктури держави.
ПЗ	–	програмне забезпечення.
Портал Дія	–	Єдиний державний вебпортал електронних послуг.
Реєстр	–	реєстр критично важливих об’єктів інфраструктури.
ЦОД	–	центр обробки даних.
ЦПД	–	Центр протидії дезінформації при РНБО України.

ВСТУП

Прогрес цифрових розробок обумовив новий вид небезпеки для людства – кібервійну. Новітні технології та Інтернет набули таких масштабів, що стали основним індикатором національної могутності, тому тепер держави світу застосовують зброю нового покоління для протистоянь в кіберпросторі.

Боротьба в цифровому форматі пропонує унікальну можливість: впровадження бажаної політики, правил і порядків без фізичного вторгнення на суверенну територію та неминучої жертви життя. Витончено продумана та запущена під контролем кібервійна позиціонується як гнучка альтернатива й одна з найефективніших стадій між санкціями та ядерними бомбами. Наслідки кібервійни можуть стати невідворотною точкою навіть для ретельно спроєктованих державних інформаційних комплексів і назавжди спричинити втрату довіри громадян до них.

На жаль, можна простежити абсолютну відсутність міжнародного діалогу та регулювання щодо стримування кібервійни та покарання за жодні з її проявів. Це дуже прикра тенденція, оскільки кіберсфера – це область, у якій інновації та операційне мистецтво значно випередили політику та стратегію.

Сьогодні інформаційний сектор України охоплює критично важливі об’єкти інфраструктури, які реалізують державну політику з метою забезпечення й підтримки цифрових й електронних життєво важливих національних інтересів. Вони, безумовно, передбачають наявність і функціонування систем з невпинними потоками інформації з обмеженим доступом, циркуляція у кіберпросторі яких породжує нові й нові загрози кібербезпеці держави.

Бути частиною кіберпростору – ставати для когось мішенню. Кібервплив завжди направлений на людину, у розглядуваній площині даної роботи – на найслабший елемент систем Supervisory Control And Data Acquisition (далі – SCADA), тобто об’єкта критичної інформаційної інфраструктури. Усі досягнення цифрового світу приваблюють кожну особистість і всебічно проникають у її повсякденне життя. Натомість для поточної ситуації України віртуальний створив

загрозу для виконання людиною обов'язків, пов'язаних із забезпеченням сталого функціонування державних потужностей. У вирі кібервійни, де громадяни України постали жертвами російської пропаганди, соціальні мережі виступили ворогом для наших співвітчизників. Нездатність розібратися з напливом гігантських потоків інформації, просочених пропагандою, у такій критичній ситуації могла б обернутися цифровою пасткою для українців, проте влада провела масштабні роботи й мінімізувала фактично до 10% поширення операцій кібервпливу.

Оскільки кібервійна ще триває, як і повномасштабне російське вторгнення, представники уряду України, відповідальні за захист громадян у цифровому середовищі, утримуються від розповсюдження даних про залучені сили (країни, міжнародні компанії, виробничі потужності) та їх внесок у підтримку злагодженості роботи й чистоти кіберпростору, проте офіційні заяви представників влади й результати роботи у відкритих джерелах дають змогу визначити, які заходи виявилися найнеобхіднішими для громадян та що слід робити надалі. Інформаційний сектор як складова критичної інфраструктури виявився неабияк вразливим у цій кібервійні через атаки на його ресурси, тому недопущення кіберпливу на його співробітників, як і для всіх громадян, стало масштабним і всеохоплюючим завданням.

Таким чином, розробка комплексу заходів щодо захисту інформаційного сектору держави від кібервпливу під час кібервійни буде здійснюватися шляхом дослідження, аналізу та доопрацювання впроваджених напрямків роботи з кібербезпеки владою України протягом російського вторгнення на територію нашої держави у 2022 році.

Початкові результати роботи в цьому напрямку були висвітлені під час Міжнародної науково-практичної конференції «Прикладні інформаційні системи та технології в інформаційному суспільстві» (AISTIS-V) від 30 вересня 2021 року в тезах «Forecasting cyberimpact on information sector of the state as a preventive method of protection against cyberwar».

Актуальність обраної теми дипломної роботи є безперечною, враховуючи розв'язану Російською Федерацією повноцінну гібридну війну та відсутність

цілісного, конкретного та всебічного регулювання джерел інформації під час кібервійни як частини гібридної війни, які становлять негативний вплив на персонал критично важливих об’єктів інфраструктури країни-жертви.

Метою дипломної роботи є провести дослідження небезпечного кібервпливу на суспільство (державу) під час гібридної війни та розробити відповідний захист інформаційного сектору держави.

Для досягнення зазначеної мети поставлено наступні **завдання**:

- розкрити необхідність захисту критичної інфраструктури в умовах кібервійни;
- простежити глобальні та локальні події, які стали передумовами кібервійни в українському віртуальному просторі;
- виконати аналіз заходів влади щодо забезпечення захисту інформаційного сектору;
- розробити комплекс заходів захисту від кібервпливу на персонал критично важливих об’єктів інфраструктури на основі такого, що відбувався протягом російського вторгнення на територію України з лютого по травень у 2022 році.

Об’єктом дослідження є процес здійснення кібервпливу на працівників критично важливих об’єктів інфраструктури інформаційного сектору.

Предметом дослідження є сукупність заходів для протидії кібервпливу на працівників критично важливих об’єктів інфраструктури інформаційного сектору.

Методи дослідження: системний аналіз, історичний метод, ізолювання, узагальнення, абстрагування.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ НЕОБХІДНОСТІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРВІЙНИ

1.1 Розгляд поняття «критична інфраструктура»

Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII було офіційно закріплено два надзвичайно важливі поняття, які, безумовно, рівноправно займають місце в системі захисту кіберпростору України – «критично важливий об’єкт інфраструктури» та «об’єкт критичної інформаційної інфраструктури».

Верховна Рада України ухвалила, що всі установи на території України приватної, державної чи комунальної форми власності є критично важливими об’єктами інфраструктури (далі – КВОІ), якщо їх функціонування ґрунтується на виробництві таких технологічних процесів або послуг, без яких не буде стабільної роботи економіки, підприємств промисловості, надійної життєдіяльності суспільства та безпеки громадян. Також обов’язковою умовою є те, що в разі порушення нормального виконання обов’язків такими установами через їх псування або руйнування відбудеться поширення негативних наслідків на системи національної безпеки і оборони України, екології, матеріального забезпечення та/або виникне небезпека для життя і здоров’я людей [1]. Таким чином, під поняттям «критичної інфраструктури» (далі – КІ) розглянемо сукупність таких об’єктів.

Невід’ємною частиною до поняття, розглянутого вище, є об’єкти критичної інформаційної інфраструктури (далі – ОКІІ), сутність яких полягає в започаткуванні певної системи або взаємопов’язаних систем, які будуть виконувати комунікаційні або технологічні функції в середовищі КВОІ. Система володітиме такою категорією тільки тоді, якщо кібератаки на неї будуть загрозою для порушення стабільної роботи КВОІ, на якому вона працює [1].

Визначення, яка інфраструктура є критичною для підтримки безперервних послуг та сервісів, до яких типів загроз чи небезпек вона вразлива та її перелік, є стратегічним завданням для безпеки України. Віднесення ресурсів до цієї категорії інфраструктури є пріоритетом на шляху до зміцнення безпеки країни, оскільки це допоможе вжити всіх необхідних заходів для підвищення стійкості КВОІ і зменшення ймовірності реалізації їх ризиків.

1.2 Вплив стану критичної інфраструктури на національну безпеку

Держави та їх громадяни покладаються на інфраструктуру. Сучасне суспільство цілком залежить від електрики та транспортних систем, банківських і телекомунікаційних, поштових і судноплавних послуг, а також різноманітних додаткових сервісів, які забезпечують безперервність життя та дозволяють людству процвітати [2]. Порушення роботи таких служб може спричинити масові невдоволення, дефіцит комфорту та фінансові втрати цивільним особам, компаніям та уряду. Виведення з ладу або руйнування інфраструктури може не тільки спричинити незручності, а й знизити здатність держави захищати себе як від внутрішніх, так і від зовнішніх загроз, завдати значної економічної шкоди, викликати соціальні заворушення і навіть призвести до втрати людей. Тому захист такої інфраструктури, особливо тієї, яка вважається критичною, є очевидним стратегічним завданням й обов’язком будь-якої суверенної держави.

Хоча потреба в захисті критичної інфраструктури далеко не нова, діджиталізація ставить перед собою нові виклики. У доцифровому світі роль уряду у захисті інфраструктури була відносно виправданою та простою, оскільки ризики виникали й матеріалізувалися в кінетичній сфері [2]. Таким чином, відповідні державні та приватні структури, які контролювали інфраструктуру, могли зосередитися на забезпеченні фізичної безпеки шляхом підвищення її стійкості проти заподіяння шкоди та шляхом інвестування в захисні та оборонні заходи від цих добре відомих (якщо не передбачуваних) ризиків.

Поширення цифрової ери суттєво змінило та переконструювало загрози, з якими стикаються об’єкти КІ, і форми відповідних необхідних заходів. Критична інфраструктура тепер покладається на цифрові системи, такі як SCADA. У деяких випадках ці системи мають віддалений доступ і навіть автоматично керують КІ [3]. Ці та інші технології, що використовуються для моніторингу та роботи КІ, безсумнівно, покращують її функціональність та створюють величезну соціальну корисність. Проте використання цифрових заходів наражає критичну інфраструктуру, а отже державу та суспільство загалом, підвищеним ризикам – ризикам кіберпростору.

Такі загрози можуть матеріалізуватися як з цифровими, так і з кінетичними негативними наслідками. Іншими словами, вони можуть проявлятися у втраті даних, несправності комп’ютеризованої платформи або пошкодженні електричних мереж, систем поїздів або каналізаційних установок. Тому захист КІ від кіберзагроз є проблемою національного значення, якою стурбовані не лише представники влади, а й громадськість у цілому.

1.3 SCADA як чутлива частина критично важливих об’єктів інфраструктури

Саме системи диспетчерського управління та збору даних – SCADA – сьогодні повсюдно забезпечують надійну роботу сучасної інфраструктури. Вони становлять сукупність безпосередньо об’єктів критичної інформаційної інфраструктури або їх окремі складові, оскільки представляють автоматизований контроль та дистанційний моніторинг процесів у реальному світі. Викликом виступає налаштування таких систем достатньо гнучко та безпечно, відстежувано та керовано, щоб запобігти підвищенню ризиків як через операційні помилки, так і через інциденти кіберпростору, включаючи вторгнення та зловмисне програмне забезпечення (далі – ПЗ), що може поставити під загрозу їхню роботу чи призвести до катастрофи.

SCADA розгорнуті у всьому світі на об’єктах КІ, від виробництва електроенергії до громадського транспорту та промислових комплексів. Від забезпечення своєчасного руху поїздів до забезпечення правильної температури ядерних реакторів системи SCADA підтримують необхідні аспекти нашого повсякденного життя і в багатьох випадках мають вирішальне значення для благополуччя та існування вітчизняної економіки [4]. Хоча ці системи, як правило, спроєктовані так, щоб бути надійними та безвідмовними, кількість порушень безпеки за останнє десятиліття показує, що їхнє початкове планування та подальша еволюція не врахували належним чином ризики навмисної атаки. КІ характеризується взаємозалежністю (фізичною, кібернетичною, географічною та логічною) та складністю взаємодіючих компонентів, тому принципи та процеси управління інформаційною безпекою треба застосовувати до всіх систем SCADA без винятку.

Розглядаючи архітектуру SCADA, необхідно зауважити, що це спеціалізовані поєднання комп’ютерних мереж і пристроїв, які узгоджено працюють для моніторингу та контролю ключових процесів, пов’язаних із керуванням машинами, обладнанням та об’єктами [4]. Вимірювання, отримані з різних датчиків (температура, тиск, витрата тощо), використовуються, наприклад, для прийняття рішень: відкрити клапан і випустити воду з резервуара, коли він заповниться, або ініціювати аварійне відключення атомної електростанції. Системи SCADA зазвичай розгортаються в трьох основних сферах [5]:

1) управління промисловими процесами – контроль хімічних процесів, генерація електроенергії, нафтопереробка;

2) управління інфраструктурою – очищення та розподілення води, керування нафто- та газопроводами, масштабними системами зв’язку;

3) управління об’єктами – адміністрування офісу, центру обробки даних (далі – ЦОД), аеропорту, корабля; моніторинг і контроль опалення, вентиляції та кондиціювання повітря, фізичний доступ та споживання енергії.

Управлінська інформація та звіти передаються до та від пристроїв SCADA через такі інтерфейси, Рис. 1.1, [5]:

- Людино-машинний інтерфейс, Human Machine Interfaces (далі – HMI) – дозволяє оператору переглядати стан процесів та реагувати на них.
- Система нагляду – комп’ютери, які відстежують і відправляють команди для керування пристроями та процесами.
- Термінальні блоки, Remote terminal units (далі – RTU), перетворюють сигнали від датчиків процесу в цифрові дані та передають їх у систему нагляду.
- Комунікаційна інфраструктура – з’єднує RTU із системою нагляду.

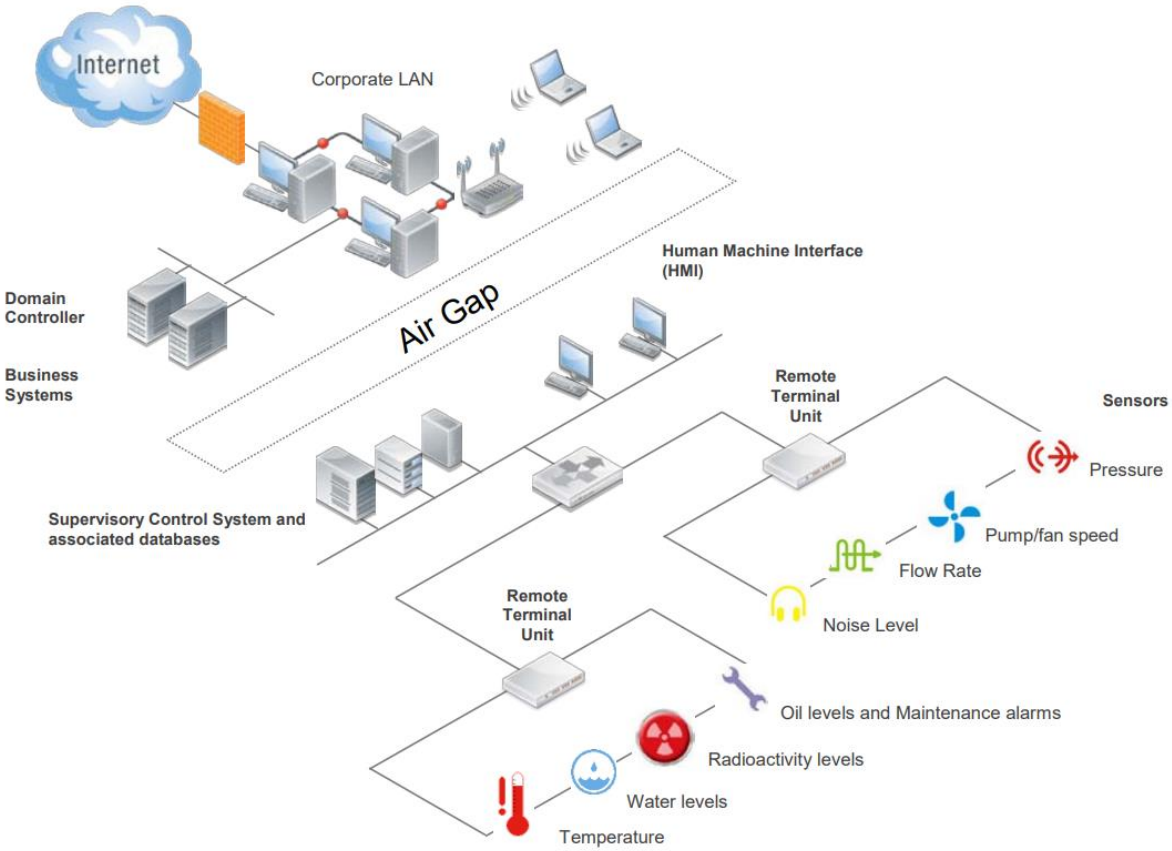

Рисунок 1.1 – Промислова система управління з мережевою архітектурою SCADA

Традиційно мережі SCADA були відокремлені від інших корпоративних мереж, щоб мінімізувати доступ до незахищених областей, таких як Інтернет. Однак останнім часом все більше організацій підключають мережі SCADA до інших потенційно незахищених мереж, щоб скоротити витрати, поділитися оперативною інформацією або розповсюдити дані замовлень і розрахунків. Навіть якщо підключення мереж SCADA до інших мереж заборонено корпоративною політикою,

неправильно встановлені системи можуть ненавмисно об’єднати мережі, що наражає на небезпеку їх та процеси, які вони контролюють.

Вплив атак, спрямованих на SCADA, залежить від намірів зловмисників та рівня їх доступу та знань про мету. Втрата доступу або неправильне використання таких систем може призвести до серйозних фізичних пошкоджень, збоїв і фінансових збитків компанії. Зловмисники можуть використовувати свій доступ до SCADA-систем для збору інформації, такої як план об’єкта, критичні пороги або налаштування пристрою для використання в потенційних атаках. Саботаж, у тому числі порушення роботи служб або створення небезпечних і навіть смертельних ситуацій, пов’язаних із горючими або критично важливими ресурсами, є загрозливою крайністю.

Зловмисники отримують доступ над SCADA-системами різними способами, одним з яких є використання недоліків людино-машинних інтерфейсів. HMI визначають як місце, де дані обробляються і надаються для дослідження та контролю оператором. Цей інтерфейс зазвичай включає елементи керування, за допомогою яких користувач може взаємодіяти із системою, надсилаючи команди машинам. Сучасний HMI забезпечує розширену і налаштовану візуалізацію поточного стану системи. Інтерфейс часто встановлюється у підключеному до мережі місці, проте його слід встановлювати лише в ізольованій надійній мережі [5].

HMI забезпечує спрощений спосіб моніторингу декількох RTU або програмованих логічних контролерів. Інтерфейс зазвичай пов’язаний з базами даних та ПЗ системи SCADA для надання тенденцій, діагностичних даних та управлінських відомостей, серед яких процедури планового обслуговування, логістична інформація, докладні схеми для конкретного датчика або машини, а також процедури з усунення несправностей [6]. HMI в SCADA необхідно розглядати як найціннішу мету для супротивника, оскільки успішно отримавши доступ до нього, зловмисник фактично володіє всією мережею SCADA.

Людина є найслабшим механізмом у забезпеченні мір захисту, тому власне оператор HMI представляє величезну загрозу для всього КВОІ. В умовах кібервійни від поглядів, ясності розуму та політичної позиції оператора залежить безперебійне

та стале функціонування такого ОКІІ. Надсилання сигналів про «вимкнення» та «увімкнення» обладнання, яке виконує різноманітні процеси, їх зупинка або неправильне налаштування, зумовлені недобросовісністю користувача, можуть стати тактичним або навіть стратегічним провалом і надати перевагу супротивнику уже не тільки на цифровому, а й на кінетичному фронті.

1.4 Модель Лімби, Плети, Агафонова і Дамкуса

У 2017 році литовські дослідники Тадас Лімба, Костянтин Агафонов, Мартинас Дамкус з Університету Миколаса Ромерісата у Вільнюсі та Томаш Плета з Центру передового досвіду з енергетичної безпеки НАТО запропонували новітню модель управління кібербезпекою, яку можна використовувати для забезпечення безпеки будь-якої критичної інфраструктури, а також для покращення стану кібербезпеки бізнес-компанії чи урядової організації. Вони не стали зосереджуватися на впровадженні конкретного технологічного обладнання або процесів управління інформаційною безпекою, які використовуються для підвищення безпеки критичної інфраструктури, а надали основну інформацію про запропоновану модель, Рис. 1.2, [7].

Рисунок 1.2 – Модель управління кібербезпекою литовських науковців

Представлена модель побудована на основі шести основних галузей, які, на думку авторів, є найбільш критичними в процесі забезпечення кібербезпеки. Усі ці елементи мають однакову важливість, і їх необхідно розвивати на об’єкті разом, тому що розробка лише одного сегменту моделі не внесе жодних серйозних змін у стан його безпеки.

Розглянемо кожну з секцій детальніше:

1. Правове регулювання – частина моделі, яка побудована на основі вимог, юридичних процедур й аспектів, яких має досягти організація в процесі забезпечення заходів з кібербезпеки [7]. Секція повинна містити всі законодавчі акти, які будуть використовуватися в повсякденному житті організації (інструкції з безпеки для співробітників, офіцерів інформаційної безпеки та адміністраторів мережі, стандарти, які використовуються або планується розробити в організації).

2. Належне управління – частина моделі, яка з точки зору досягнення кібербезпеки, найважливіша. Кожен сучасний керівник повинен знати основні цілі кібербезпеки у своїй організації та розуміти, що існують ризики, які ніколи не будуть виключені з функціонування організації. Керівництво повинно прийняти той факт, що неможливо уникнути всіх загроз, але можна мінімізувати вплив кіберінцидентів на організацію, якщо вони трапляються [7]. Будь-який проєкт або діяльність, яка планується в організації, спочатку мають бути повністю розглянуті з точки зору безпеки, і це допоможе заощадити гроші та ресурси.

3. Управління ризиками – це здатність організації правильно визначати ризики, які виникають навколо організації, і гарантувати, що вони мають спеціальні засоби, щоб контролювати вплив цих ризиків. Як зазначалося раніше, організації не можуть уникнути всіх ризиків [7]. Іноді важливіше виявити всі ризики та мати план на випадок надзвичайних ситуацій, ніж намагатися їх усіх уникнути. Крім того, організація повинна навчитися не тільки уникати ризиків, а й приймати їх.

4. Культуру безпеки в установі можна вважати найважчим етапом для реалізації та контролю. В автоматизованих засобах безпеки можна використовувати інформаційні технології, математику чи моделі управління ризиками, щоб спробувати розрахувати, передбачати та запобігти небезпечним ситуаціям, але з

персоналом набагато складніше, оскільки людей неможливо запрограмувати на точне й бездоганне виконання обов’язків та дотримання всіх вимог. Цей аспект дуже важливий, і організація повинна розуміти, що її вразливість може бути зумовлена співробітниками, які в ній працюють. Безпека повинна бути зрозумілою для кожного члена організації, і весь персонал повинен навчитися захищати організацію та себе від інцидентів кібербезпеки, оскільки помилки можуть мати вирішальне значення для стану захисту установи [7]. Одна з найбільших помилок кібербезпеки в цьому вимірі зазвичай пов’язана з думкою вищих керівників та ІТ-спеціалістів, що вони повинні мати більше привілеїв і доступу до своїх систем, ніж це насправді вимагається посадовими обов’язками, проте таке уявлення може поставити під загрозу усі виконані роботи з кібербезпеки.

5. Управління технологіями – це процес, який запроваджує зручніші механізми для застосування технологічного підходу в процесі досягнення організаційних цілей. Ресурси ІТ дозволять відслідковувати, чи є компоненти в організації вразливими чи пошкоджені. Таким чином, керування технологіями та компонентами дозволить скоротити час, необхідний для усунення наслідків інциденту безпеки або запобігання повторення інциденту безпеки [7].

6. Управління інцидентами – це частина, що тісно пов’язана з правовою секцією моделі, яка регламентує, що організація повинна мати спеціальні плани щодо керування наслідками інциденту. Такі процедури включатимуть інструкції для членів установи, які необхідно застосувати у разі випадку з безпеки. Також потрібно визначити, які заходи необхідно вжити, намагаючись зменшити негативний вплив інциденту, і як відновити нормальну роботу організації [7].

Кожен вимір запропонованої моделі управління кібербезпекою має бути чітко окреслений, проаналізований та оцінений, а організація повинна розробити чіткий план щодо усунення проблем, які виявлені в кожній області.

Загалом, реалізація секцій моделі управління кібербезпекою в організації мінімізує ризики щодо кібератак та обмежує їх руйнівний вплив на критичну інфраструктуру. Така розробка допоможе краще зрозуміти ситуацію безпеки навколо установи та всередині неї, оскільки її вимоги виявлять вразливі місця

організації, тенденції кіберзлочинності та атак. Безумовно, впровадження моделі забезпечить ефективніші шляхи комунікації всередині організації, а також покращить взаємодію з партнерами шляхом підвищення репутації і стійкості проти нападів хакерів.

Отже, необхідність захисту критичної інфраструктури розглянута та підтверджена. Спосіб організації SCADA-систем створює для національної безпеки величезні загрози через наявність у ній операторів. Також модель литовських дослідників визнає, що саме людина є найскладнішим елементом для контролю на критично важливому об’єкті інфраструктури, а тому вона створює високі ризики для його компрометації.

РОЗДІЛ 2
ПЕРЕДУМОВИ РОЗГОРТАННЯ КІБЕРВІЙНИ В УКРАЇНСЬКОМУ ВІРТУАЛЬНОМУ ПРОСТОРІ

2.1 Кібервійна як засіб досягнення політичної переваги

Загроза кібервійни затьмарює уявлення про спокійне та безпечне майбутнє: нова форма конфлікту спроможна подолати кордони в будь-яку сторону світу та телепортувати хаос війни до мирних громадян за тисячі кілометрів від її фронту.

Зовсім недавно міркування про кібервійну починалися з неймовірних гіпотез: чи може держава спонсорувати хакерів, аби ті розгорнули масові атаки проти систем ворогів? Вивели з ладу сервери банків і заморозили банкомати на території країни опонента? Заблокували доступ до мереж і баз даних судноплавних фірм, нафтопереробних заводів чи фабрик промислового масштабу? Ввели шкідливе програмне забезпечення до систем аеропортів та лікарень?

На жаль, у реаліях XXI століття такі сценарії більше не розглядають як гіпотетичні: кожна з цих подій відбулася насправді і їх кількість зростає з кожною секундою. Інциденти у віртуальному просторі шокують своїми руйнівними наслідками кожного разу, і вже точно можна сказати, що кібервійна залишила сторінки наукової фантастики і детально розроблені платформи військових ігор, щоб стати реальністю і тримати в страху всю планету. Загроза нападу виходить за межі вандалізму, кримінального спекулювання і навіть шпигунства і містить форми руйнування фізичного світу, які зовсім нещодавно можна було здійснити лише за допомогою військових атак і терористичного саботажу.

Найбільш тривожним є те, що засоби та методи кібервійни зосереджені у таких країнах, як Іран, Північна Корея та Росія, оскільки вони впроваджують нові руйнівні форми кібератак, а США та інші держави-учасники «Five Eyes», ймовірно, володіють найсучаснішими можливостями кібервійни у світі, але, судячи з опублікованих відомостей, демонстрували більшу стриманість [8]. «Five eyes»

відноситься до тісного партнерства з обміну розвідувальними даними між Австралією, Канадою, Новою Зеландією, Великобританією та США, яке виникло в результаті двостороннього поширення такою інформацією між США і Великобританією під час Другої світової війни. Партнерство передбачає тісну співпрацю між розвідувальними службами п’яти країн та тісні зв’язки між іншими службами безпеки, спеціальними органами та поліції, що й виступає прикладом політичної переваги на міжнародній арені серед об’єднань країн.

2.1.1 Історія та значення кібервійни

Для осягання унікальної загрози кібервійни варто спочатку окреслити її рамки та терміни для єдиного трактування і політиками, і військовими, і IT-інженерами. Лише протягом останніх десятиліть еволюції термін «кібервійна» досяг свого справжнього тлумачення.

Історія всієї кібернетики Томаса Ріда, описана в книзі «Rise of the Machines», «Повстання машин», затьмарила істинне значення терміну: вперше цей твір з’явився у статті журналу «Omni» 1987 року, у якому прогнозувалися війни з гігантськими роботами, геніальними літаючими апаратами та керованими системами зброї. Уже в 1990-х роках замість фантазій війни з роботами з’явилася ідея, фокус якої був направлений на взаємодію комп’ютерів з Інтернетом для впливу на нормальний порядок людства. У 1993 році з’явилася стаття «Cyberwar is Coming!», «Кібервійна наближається!», авторами якої стали два науковці з аналітичного центру RAND. Ці матеріали правдоподібно описували сценарій, у якому в найближчі роки будуть найматися військові хакери в стратегічних політичних цілях. Їхні сили будуть спрямовані на розвідку та проникнення у ворожі комп’ютери для порушення роботи систем противника і керування ними задля здобуття політичної переваги [8].

Тим часом, з огляду на подальший розвиток технологій, аналітики RAND зробили висновок, що військові хакери можуть мати набагато більший руйнівний вплив на ворожі потужності. Такі спеціалісти зосереджують у своїх руках величезну владу, оскільки мають змогу атакувати комп’ютеризовані й автоматизовані

елементи критичної інфраструктури ворога, і ці діяння матимуть потенційно катастрофічні наслідки для цивільного населення: у світі, який все більше залежить від комп'ютерів, це може означати виснажливий саботаж проти залізниць, фондових бірж, авіакомпаній і навіть електричної мережі [8].

Хакерство не можна розглядати лише як певну тактику на периферії війни – кібератаки є повноцінною зброєю для дестабілізації противника. Колишній президент США Білл Клінтон також схилявся до такого твердження, коли у 2001 році у своїй промові повідомляв, що «сьогодні наші критичні системи, від силових структур до управління повітряним рухом, пов'язані і керуються комп'ютерами» і потім продовжив: «Хтось може сидіти на тому самому комп'ютері, зламати комп'ютерну систему та потенційно паралізувати компанію, місто чи уряд». Відтоді ця первинна інтерпретація кібервійни була ретельніше досліджена, і найбільш чітко її виклали в книзі 2010 року «Cyber War: The Next Threat to National Security and What to Do About It», «Кібервійна: наступна загроза національній безпеці та що з нею робити» Річард Кларк, радник з національної безпеки колишніх президентів, і Роберт Кнейк, який пізніше служив радником президента Обами з кібербезпеки [8].

Безпосередньо Кларк і Кнейк визначили кібервійну як дії держави, направлені на проникнення в комп'ютери або мережі іншої країни, щоб заподіяти шкоду чи збій. Але поки автори досліджували це визначення, світ уже зазнав на гіркому досвіді, що цифрові атаки можуть вийти за межі простих комп'ютерів і мати реальні фізичні наслідки.

Саме в Естонії, найбільш пов'язаній комунікаціями країні на той час, відбулася перша історична подія, яка могла б достовірно відповідати визначенню Кларка і Кнейка. Її охрестили як «Web War I» і відбулася вона за декілька років до випуску книги, яка була згадана вище [8]. Навесні 2007 року безпрецедентна серія DDoS атак вразила понад сотню естонських веб-сайтів і нанесла збитків онлайн-банкінгу країни, цифровим засобів масової інформації (далі – ЗМІ), державним сайтам та популярним веб-ресурсам. До цих нападів призвело рішення уряду Естонії прибрати пам'ятник радянських часів із центральної частини Таллінна, що викликало гнів російськомовної меншини в країні та призвело до протестів на

вулицях міста та в Інтернеті. Кібератаки тривали тижнями і походили з бот-мереж – сукупності ПК по всьому світу, захоплених зловмисним програмним забезпеченням, які належали організованим російським кіберзлочинним групам.

Наступного року російський уряд усе частіше і не безпричинно пов'язували з політично мотивованими кібератаками. Подібний потік DDoS-атак вразив десятки веб-сайтів в іншій країні поруч з Росією – Грузії. Цього разу кібератаки супроводжували реальне фізичне вторгнення: відбувся російський напад з метою «захисту» дружніх до Росії сепаратистів у межах Грузії разом із танками, які рухалися до Тбілісі, і російським флотом, який блокував узбережжя країни на Чорному морі. Цифрові атаки в цьому випадку дестабілізували конкретні міста безпосередньо перед прибуттям підрозділів солдатів, що допомогло поєднати атаки у віртуальному та реальному просторах [8].

Світова концепція кібервійни назавжди змінилася в 2010 році. В охоронній фірмі VirusBlokAda стався інцидент, де спеціалісти з кібербезпеки ідентифікували невідомого походження блок коду шкідливого ПЗ, який вразив комп'ютери з активним антивірусом. Аналітики назвали цю програму Stuxnet і, дослідивши її, зробили висновок, що це найскладніший фрагмент коду, що був замішений у кібератаках до цього часу, і що він був спеціально розроблений для знищення центрифуг на ядерних установках Ірану.

Протягом 2009 та 2010 років Stuxnet знищив понад тисячу алюмінієвих центрифуг, які були встановлені на іранському підземному ядерному збагачувальному заводі в Натанзі. Об'єкт фактично став неконтрольованим через плутанину та хаос. Обійшовши іранську мережу програма ввела команди в так звані програмовані логічні контролери, що керували центрифугами, прискорюючи їх або маніпулюючи тиском всередині них, поки вони не розірвалися на частини [8]. Як наслідок, світова спільнота визнала Stuxnet першою кібератакою, коли-небудь розробленою для безпосереднього пошкодження фізичного обладнання, і актом кібервійни, який наніс руйнівний вплив на ресурси. Після цієї події і почалося нарощування ресурсів для глобальної гонитви кіберозброєнь.

Найближчим часом Іран виступив сам безпосередньо як агресор, а не жертва, для помсти та досягнення економічної переваги серед країн свого регіону. У серпні 2012 року саудівська фірма Saudi Aramco, одна з найпотужніших у світі виробників нафти, була вражена шкідливим програмним забезпеченням, відомим як Shamoon. Було знищено три чверті пристроїв компанії, тобто приблизно 35 000 комп'ютерів, і це призвело до паралізації діяльності підприємства. На екранах покалічених машин зловмисне ПЗ залишило зображення палаючого американського прапора [8].

Уже наступного місяця нова група іранських хакерів під назвою Operation Ababil вразила всі великі банки США, виводячи з ладу їхні веб-сайти за допомогою неперервних DDoS-атак. Можна вважати, що такий вплив на ресурси став більш цілеспрямованою технікою знищення, аніж та, яку росіяни використовували проти сайтів в Естонії та Грузії. Ці дії також не пройшли непоміченими, і спеціалісти віднайшли докази приналежності атаки до Ірану, незважаючи на хактивістські настрої. Своєю помстою Іран довів США, що не забуває вчинені ними руйнування.

У лютому 2014 року, через рік після розглянутих атак, іранські хакери знову атакувати американські ресурси. Мільярдер Шелдон Адельсона спонукав США вразити Іран ядерною зброєю і, як наслідок, хакери у відповідь на такі заяви атакували казино Adelson в Las Vegas Sands шляхом впровадження руйнівного шкідливого ПЗ для очищення тисяч комп'ютерів, подібно до ситуації з Saudi Aramco [8].

Проте у 2014 році Іран був єдиним, хто користувався силою кібератак по всьому світу і безжально втручався в цивільний порядок. Північна Корея також стала на арену кібервійни для довершення багаторічних спроб вивести з ладу потужності Південної Кореї. Хакери глибоко проникли в мережу Sony Pictures напередодні випуску фільму «The Interview» про змову вбивства північнокорейського диктатора Кім Чен Ина. Ці зловмисники назвали себе «Вартові миру». У результаті нападу було незаконно вилучено та розповсюджено листи, а також зірвався випуск фільму. Під кінець свого рейду хакери очистили тисячі комп'ютерів і залишили на них загрозливе зображення скелета разом із повідомленням про вимагання грошей і скасування випуску «The Interview» [8].

Після завершення розслідувань ФБР публічно назвало уряд Північної Кореї виконавцем атаки, і частково це ґрунтувалося на основі китайської IP-адреси, яку, як тоді було відомо, використовували північнокорейські хакери. Таким чином, перелік учасників кіберпротистоянь зростав.

2.1.2 Кібервплив – потужна техніка кібервійни

Цифрова ера змінила спосіб спілкування всієї планети, оскільки взаємодія людей почали відбуватися через засоби онлайн-комунікації. Використовуючи соціальні мережі, такі як Facebook та Instagram, і месенджери, на кшталт WhatsApp і Telegram, кожен може підтримувати зв'язок з друзями та родиною; поширювати публікації, повідомлення, зображення та відео; ділитися досвідом та читати новини оточення. Соціальні медіа також є ефективним способом впливу на поведінку суспільства та формування громадської думки, навіть виділяються особистості інфлюенсери, тобто, фактично «ті, хто впливають», за якими стежить багатомільйонна аудиторія. Поширивши публікацію чи думку в Twitter, беручи участь у дискусії на форумі та надсилаючи сентиментальну чи політичну картину, кожен має змогу вплинути на інших, а іноді й переконати їх у своїй думці. Фактично, можна стати учасником сотень і тисяч цифрових розмов, використавши шанс вплинути на великі спільноти.

Держави завжди використовували інформацію для досягнення своїх політичних цілей, оскільки конфлікти ніколи не обмежувалися військовою сферою. У кіберпросторі психологічні маніпуляції виступають кібервпливом, що є фактично насиченою і жорсткою пропагандою. Використання інструментів і методів кіберпростору для маніпулювання громадською думкою називається операцією кібервпливу. Вона може мати різну мету: психологічно змінювати людину, підривати моральний дух, впливати на свідомість суспільства, прищеплювати неконтрольованість і неспроможність захистити свідомий спосіб життя тощо.

Сьогодні кіберпростір з його швидким розширенням постає ідеальним варіантом для проведення в ньому операцій кібервпливу, можливо, навіть кращим за

проведення руйнівних актів. Тім Стівенс, викладач глобальної безпеки британського Кінгс-коледжу, зазначив, що «кібервійна майбутнього може полягати не в зломі електричних мереж, а в злому розумів шляхом формування середовища, у якому відбуваються політичні дебати». Оскільки операції кібервпливу можуть завдати психологічної шкоди, вони також відомі як дезінформаційні кібератаки [9].

У XXI столітті практично будь-яка країна здатна використати кіберпростір, і зокрема соціальні медіа, для управління операціями кібервпливу в рамках цілісної кібервійни. Загалом більшість цих операцій виконується приховано: у випадках, коли операція виявлена, буде важко швидко визначити, хто за нею стоїть. Операції кібервпливу можуть спрямовуватися на широку громадськість за допомогою загальних заяв або можуть призначатися конкретній аудиторії чи одній єдиній людині через цільові повідомлення, щоб досягти більш ефективного враження , контролювати відповіді та реакцію.

Не тільки виявлення операцій кібервпливу є трудомістким завданням, а й конкретне їх розрізнення на легітимні й зловмисні та відслідковування наслідків. Просування продукту чи новітньої ідеї є законним, навіть як операція кібервпливу. Підбурювання, сприяння радикальним або насильницьким діям, а також втручання в процеси державного управління є прикладами зі зловмисним наміром розв’язання чи посилення кібервійни.

Операції кібервпливу стали серйозною проблемою у всьому світі, і зараз вони набули найрізноманітніших форм – фейкові новини, дезінформація, політичний астротурфінг, інформаційні атаки. Вони з’являються як компонент гібридної війни – у поєднанні з традиційними кібератаками, а також із звичайними військовими діями чи кінетичними атаками [9]. У мирний час метою операцій впливу в кіберпросторі може бути просування бажаних ідей або певних угрупувань у запланованому напрямку. Прикладом може бути політична партія, яка проводить кампанію, щоб переконати своїх виборців голосувати за неї. Якщо ті самі процедури виконає інша країна, то це, безумовно, вважатиметься втручанням у внутрішні справи суверенної держави. Під час конфлікту чи війни мета операцій кібервпливу може полягати у створенні антиурядових дискусій, настрої громадської думки проти дій чинної влади

(наприклад, її військових рішень), підриві суспільної моралі (на кшталт, створенні відчуття незахищеності) для того, аби зруйнувати впевненість у компетенції існуючої влади, її спроможності захистити населення, викорінити віру в армію та військовий потенціал, переконати в зосередженні важелів впливу в інших осіб.

Таким чином, кібервплив може бути націлений на всі верстви суспільства з використанням онлайн-баз даних або соціальних мереж. Часто це передбачає загальні заяви, які шляхом поширення на мікрорівні виконують цілі на макрорівні.

2.2 Руйнівні наслідки кібератак на українські ресурси

Незважаючи на те, що північнокорейські та іранські хакери влаштовували віртуальний хаос з величезними втратами, на кшталт атак проти Las Vegas Sands і Sony Pictures, кіберпротистояння 2014 року були обмежені поодинокими інцидентами та періодичними актами зриву. Однак у той же час Україна переживала Революцію Гідності, після якої відбулося російське вторгнення. Ці події заклали основу для кібервійни.

Восени 2015 року, уже після жорстоких подій, коли під керуванням російської влади війська анексували український Кримський півострів і прослизнули через східний кордон України, щоб згуртувати проросійський сепаратистський рух у регіоні Донбасу, спеціалісти російської розвідки почали серію кібератак, використовуючи у якості зброї зловмисне програмне забезпечення. Було проведено цифрові напади на українські ЗМІ та інфраструктуру, зокрема національну залізницю та аеропорт Києва, завдавши непоправної шкоди комп’ютерам.

Потім, за день до Різдва, ті самі хакери здійснили більш шокуючий і безпрецедентний акт саботажу: три українські регіональні енергетичні компанії стали жертвами кібератаки, що призвело до відключення світла близько 225 000 мирним жителям. Ця подія стала першим відомим випадком позбавлення електроенергії в історії через нездатність протистояти руйнівному хакерському втручанню. Відключення тривало всього шість годин, але воно стало потужним

сигналом українській владі про вразливість держави до віддалених атак, а також усій світовій спільноті про те, що російські хакери здатні до нищівних нападів [10].

Війна досі тривала, і наприкінці 2016 року російські хакери розпочали чергову серію кібератак, набагато ширших й нахабніших, оскільки сили було спрямовано на офіційні ресурси держорганів та КВОІ. Застосувавши вдосконалену віртуальну зброю, вони отримали доступ до Пенсійного фонду, Міноборони, Казначейства та Міністерства фінансів, видаливши терабайти даних, які включали навіть бюджет, складений на наступний рік. Хакери також дібралися до залізничної компанії, зламавши її систему онлайн-бронювання на кілька днів.

Потім за тиждень до Різдва кіберзлочинці спровокували чергове відключення світла, цього разу в Києві. Атака позбавила сталого функціонування лише частину системи постачання електроенергії міста на одну годину, але зробила це, вдаривши передавальні станції, а не розподільні підстанції, як це було роком раніше; тобто експлуатували ціль, яка могла спричинити набагато більш поширене відключення світла. У цьому другому нападі використовувався новий, зловісний інструмент, який аналітики з безпеки назвали Industroyer або Crash Override [10]. Ця спеціально створена шкідлива програма була розроблена для відправлення швидких команд безпосередньо на автоматичні вимикачі в утиліті жертви, автоматизуючи процес відключення живлення. Таке російське ПЗ стало першим зразком коду, виявленим з часів Stuxnet, який був націлений безпосередньо на фізичне обладнання.

Наприкінці червня 2017 року російські хакери використали зламані сервери української бухгалтерської фірми Linkos Group, щоб виштовхнути фрагмент коду, який згодом отримав назву NotPetya. Об’єднавши хакерську програму EternalBlue з інструментом для крадіжки паролів Mimikatz в автоматизованого хробака, він майже миттєво поширився приблизно на 10 відсотків всіх комп’ютерів в Україні, зашифрувавши їх вміст деструктивним корисним навантаженням [10]. Воно було замасковане під програму-вимагач, але без механізму фактичного розшифрування файлів після того, як жертва заплатила викуп (спочатку здавалося, що це стара версія такого ж типу програми Petya, але це не так – звідси її назва). По всій Україні було порушено таким чином роботу банків, банкоматів та систем торгових точок,

паралізувавши майже всі державні установи країни та завдавши шкоди інфраструктурі, такій як аеропорти та залізниці, а також лікарні, національне поштове відділення та навіть операції з моніторингу рівнів радіоактивності на території поблизу Чорнобильської АЕС.

Вірулентність NotPetya не обмежувалася національними кордонами, оскільки було завдано збитків A.P. Møller-Maersk, найбільшій у світі судноплавній компанії; фармацевтичній компанії США Merck; французькій будівельній компанії Saint-Gobain; виробнику продуктів харчування Mondelez та виробнику побутової хімії Reckitt Benckiser. У кожному з цих випадків вірус перенасичував мережі, руйнуючі тисячі комп'ютерів та спричиняючи втрат у розмірі сотні мільйонів доларів для поточного бізнесу та витрат на відновлення. Він вразив як мінімум дві лікарні в США і закрив компанію Nuance з розробки ПЗ. NotPetya навіть поширився назад до Росії, завдавши додаткових побічних збитків таким жертвам, як державна нафтова компанія «Роснефть», виробник сталі Evraz та компанія медичних технологій Invitro. Загалом, за оцінкою Білого дому, вартість спричинених втрат NotPetya оцінювалася у 10 мільярдів доларів, хоча повний розмір непрямих збитків, можливо, ніколи не буде відомий.

2.3 Настрої держав щодо обмеження засобів кібервійни

Будь-який аналітик підтвердить те, що такі хакерські атаки не залишаться одноразовими катастрофами в історії кібервійни. Зрештою, всього за місяць до хробака NotPetya північнокорейські хакери запустили свого власного хробака-вимагача, відомого як WannaCry, який був майже таким же руйнівним. Він відключив такі мережі, як китайські університети, індійські поліцейські управління і, навіть, британську національну службу охорони здоров'я.

Є докази того, що майбутні кібератаки можуть спричинити ще більше руйнувань або навіть фізичне знищення. У серпні 2017 року зловмисне програмне забезпечення під назвою Triton (також називають Trisis) стало причиною зупинки нафтопереробного заводу, що належить саудівській фірмі Petro Rabigh. Після

місяців реверс-інжинірингу офіцери з безпеки визначили, що шкідливий код насправді не мав мети викликати зупинку, а натомість був призначений для вимкнення так званих систем безпеки заводу – обладнання, яке служить останнім технологічним захистом для запобігання небезпечним умовам, наприклад, підвищення температури або тиску. Неконтрольоване використання цих систем могло призвести до потенційно смертельних нещасних випадків, таких як вибух або витік газу [10].

З огляду на це, здавалося б, невблаганне зростання руйнівного потенціалу кібервійни, як людям подолати хаотичне майбутнє нескінченних широко поширених цифрових конфліктів? Найочевиднішою відповіддю є, звичайно, посилений стан кібербезпеки: власники КІ в уряді та приватному секторі, безумовно, могли б інвестувати більше у вдосконалення своїх мереж, відокремлюючи життєво важливі системи від Інтернету, де це можливо. Але в кібервійні також потрібно пам’ятати, що жодна технологія безпеки не зможе запобігти всі майбутні кібератаки.

Уявлення щодо кібервійни також трактують, що погрози санкційного характеру також мають важливу роль у стримуванні агресії. Країни повинні зіткнутися з серйозними наслідками, оскільки вони наважилися запустити кібератаку, яка порушує певні червоні лінії, що визначають глобальні норми прийнятної та неприйнятної хакерської діяльності. Але цих дій недостатньо, частково тому, що лінії, які прагне забезпечити міжнародна спільнота, все ще проводяться. Протягом десятиліття політики з питань цифрового захисту марно закликають до глобального договору чи конвенції, які могли б встановити правила для кібервійни.

У своїй книзі Кларк і Кнейк запропонували договір про обмеження кібервійни, який забороняв би атаки на критичну інфраструктуру іншої країни. Нещодавно президент Microsoft Бред Сміт закликав до цифрової Женевської конвенції, яка б накладала табу на кібератаки на цивільні цілі. Джош Корман, колишній директор Cyber Statecraft Initiative в аналітичному центрі Atlantic Council, запропонував більш сувору угоду, яку він описує як «кіберзону, заборонену для польотів» навколо лікарень, яка по суті почне процес обмеження кібервійни шляхом визнання будь-

якого небезпечного для життя нападу на медичні заклади військовим злочином. Але в міру ескалації гонки озброєнь у кібервійні жодна з цих ініціатив у галузі кіберсвіту не отримала великої підтримки [8].

Більше того, уряди не бажають підписувати угоди про заборону кібервійн, тому що вони не хочуть обмежувати свою власну свободу проводити кібератаки проти своїх ворогів. Іншими словами, світові держави досі не усвідомили, що в обміні руйнівними кібератаками вони більше втрачають, ніж отримують. Доки вони цього не зроблять, машина кібервійни котитиметься вперед, несучи на своєму небезпечному шляху не що інше, як інфраструктуру сучасної цивілізації.

2.4 Ступінь вразливості інфраструктури України до кібератак за 2022 рік

З 2017 року Україна неодноразово ставала мішенню російських кіберзловмисників, але найбільш деструктивними та масовими вони стали на початку 2022 року. У ніч з 13 на 14 січня одна з наймасовіших кібератак дестабілізувала українські ключові урядові сайти. 70 центральних і регіональних ресурсів України були паралізовані шляхом впровадження шкідливого ПЗ. За офіційними заявами Служби безпеки України витоку даних не відбулося [11]. Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) вела розслідування цього інциденту шляхом аналізу й тестування технічної інформації від постраждалих органів влади.

У рамках угоди про співробітництво Government Security Program Держспецзв'язку взаємодіє з компанією Майкрософт для з'ясування точних даних про походження атаки. За їх матеріалами, а саме за класифікацією програмних засобів для знищення даних, було встановлено, що в кількох закладах була експлуатована програма-вайпер WhisperGate для заміни відображуваної інформації на веб-сайтах державних органів влади. Такий вид незаконного втручання в систему називають дефейс-атакою, тобто хакери шляхом певних операцій отримують доступ до сервера, на якому розгорнуто сайт, і публікують там певні неправдиві дані, провокативні заклики чи наклепи. Проте аналітики Майкрософт заявляють, що

вплив цього ПЗ є значно глибшим за звичайну модифікацію даних, оскільки це лише один етап комплексної цільової атаки. Зазначений зловмисний програмний продукт знищує Master Boot Record і вміст файлів, на які він був націлений. Також Майкрософт підтвердив за власними базами даних, що подібних атак до цього часу зафіксовано не було, тобто це абсолютно унікальний випадок в історії кібербезпеки [12].

Варто зауважити, що величезні негативні наслідки було завдано в надзвичайно стислі терміни, що є явним показником наявності організованого угрупування «чорних капелюхів» з потужними ресурсами. До того ж, за свідченнями Держспецзв'язку на окремі ресурси шкода була завдана в ручному режимі.

Загалом за результатами дослідження інциденту спеціалісти з кібербезпеки заявляють про вплив трьох векторів атаки на державні ресурси. Існують докази експлуатації вразливостей OctoberCMS та Log4j. Аналітики ще розглядають Supply Chain Attack. Цей вид кібератаки реалізовується шляхом отримання нелегітимного доступу до мережі компанії через сторонніх постачальників, тобто розглядається ланцюжок постачання певного шкідливого ресурсу цільовій компанії [12].

Висувалося твердження, що за цим стоїть російська сторона, яка продовжує вести гібридну війну усіма можливими способами. І вже тоді були побоювання, що це лише перший крок перед військовим втручанням. У результаті аналізу доказів секретар Ради національної безпеки й оборони України Сергій Демедюк заявив, що зловмисне угрупування UNC1151 може стояти на чолі цієї атаки, і саме воно співпрацює зі спецслужбами Білорусі. Ця група вже була причетна до руйнівних атак проти ресурсів Польщі і країн Балтії [13].

Отже, можна впевнено сказати, що подібні атаки є засобом дестабілізації ситуації в державі, які підривають довіру громадян до влади. В тодішніх умовах напруженої ситуації біля східних кордонів України напади на офіційні електронні ресурси стали замахом на можливість донесення достовірної інформації українцям.

РОЗДІЛ 3
АНАЛІЗ ЗАХОДІВ ВЛАДИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕКТОРУ

3.1 Кібербезпека як вимога до регулювання критичної інфраструктури

Впровадження, підтримка й вдосконалення заходів із безпеки та непорушності критичної інфраструктури є спільною відповідальністю між зацікавленими сторонами – власниками та операторами КІ, а також державними установами та неурядовими структурами, включаючи галузеві асоціації. Ролі та обов'язки щодо заходів із сталого функціонування інфраструктури дуже різняться і на них впливає багато факторів, таких як [14]:

- належність до державної чи приватної власності;
- положення й стандарти в межах сектора;
- очікувані загрози та небезпеки для конкретного сектора.

Галузеві асоціації часто відіграють ключову роль у рекомендації практик, тоді як в інших секторах можуть існувати нормативні акти, які вимагають певних дій, або можливе застосування обох варіантів. Деякі сектори мають загальнодержавні або національні стандарти проєктування. Постачальники страхування можуть також накладати вимоги щодо безпеки до своїх страхувальників у деяких секторах [14].

Взаємодія та контроль на різних рівнях влади сприяє відповідальності та порядку, а також стимулює до обміну інформацією та практичним досвідом. Проаналізуємо, яким чином законодавчі документи України, фундамент для діяльності установ на території нашої держави, виконують регулювання безпечної та надійної роботи КВОІ інформаційного сектору.

Указом Президента України від 13 лютого 2017 року № 32/2017 було введено в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». Цей документ наголошує на майбутньому закріпленні на законодавчому рівні вимог

щодо кіберзахисту об’єктів критичної інформаційної інфраструктури. Ініціатива РНБО також окреслила намір визначити права й обов’язки суб’єктів з впровадження та контролю роботи засобів з кібербезпеки та власників (розпорядників) ОКІІ і безпосередньо затвердити протоколи комунікації між ними для організації дій з індикації, запобігання, припинення кібератак та кіберінцидентів. До переліку входить і розробка механізмів для усунення наслідків завданих збитків та притягнення до відповідальності за порушення вимог щодо кіберзахисту відповідних об’єктів. Таким чином, даний документ став одним із перших для визначення методів захисту об’єктів критичної інформаційної інфраструктури [15].

3.2 Започаткування Міністерства цифрової трансформації

Ще три роки тому такі поняття, як «діджиталізація державних процесів» та «цифрові послуги» були осторонь від повсякденного життя українців і вербально, і фізично, оскільки не існувало централізованої платформи для їх забезпечення. Електронний документообіг, електронне урядування, електронна взаємодія з громадянами тепер є реальністю для українців, яка стала можливою завдяки прогресивним реформам чинного Президента України. У травні 2019 року Володимир Зеленський ініціював проєкт «Держава в смартфоні», і після цього цілий ряд фундаментальних нововведень був представлений українцям.

Насамперед «Держава в смартфоні» вважається абсолютно інноваційною в Україні концепцією процесу надання електронних адміністративних послуг. Ідея використання мобільних пристроїв для процедури такої онлайн-взаємодії не є проривом у світі: саме Естонія вирізняється з-поміж інших країн надзвичайно високим рівнем модернізації державного забезпечення послугами та впровадженням електронних платформ для громадян, і такі технології заслужено роблять її одним з лідером Європейського Союзу у даній розробці. Практики Естонії було визначено керівними для створення і впровадження вітчизняного продукту, тому українська сторона направила міжнародну співпрацю на одержання досвіду від керівників існуючого естонського стандарту [16].

Влада висловила свою бачення в тому, що проєкт «Держава в смартфоні» позбавить українців від обтяжливої бюрократії та допоможе боротися з корупцією, оскільки оптимізація тривалих процедур й автоматизація функцій робить більш прозорою систему державних комунікацій. Базовим напрямком було заявлено об'єднання близько 350 реєстрів, аби кожен громадянин міг безперешкодно отримати певний витяг, довідку, сертифікат чи ліцензію. Дані реєстри і містять відповідну інформацію з обмеженим доступом, що знаходиться на серверах критично важливих об'єктів інфраструктури [17].

Владою було озвучено багато прогресивних завдань, які досі не озвучувалися, але вимагали уваги. Наприклад, у мобільному додатку має бути перелік персональних даних, які містяться в державних репозиторіях, а також функція сповіщення про намір перегляду таких даних певним органом. Щоб забезпечити необхідні ресурси та координувати роботи з реалізації такої концепції у серпні цього ж року Верховна Рада організувала Комітет з питань цифрової трансформації, а також Кабінет Міністрів України у Постанові «Деякі питання оптимізації системи центральних органів виконавчої влади» №829 від 2 вересня 2019 року шляхом реорганізації Державного агентства з питань електронного урядування України започаткував Міністерство цифрової трансформації України (далі – Мінцифри) на чолі з віцепрем'єр-міністром Михайлом Федоровим. До цього часу не було спеціалізованого органу, що мав би у своїх завданнях роботи з вдосконалення України в напрямку діджиталізації послуг та взаємодії відомств, а також виносити на засідання Кабміну акти для прийняття задля розвитку держави у віртуальному вимірі [18].

Наступним кроком було прийнято Кабміном Постанову «Питання Міністерства цифрової трансформації» № 856 від 18 вересня 2019 року, яка визначила сферу впливу Мінцифри: цей орган став відповідальним за цифровізацію економіки, державних послуг, навичок і прав громадян. Міністерство загалом почало охоплювати всі державні напрямки, аби зробити комунікацію з центральними органами виконавчої влади швидшою, зручнішою та з дотриманням усіх правочинів для фізичних чи юридичних осіб. Молодий орган виступив також за

оптимізацію роботи державних органів, забезпечивши принцип інтероперабельності: умови, за яких ресурси з різноманітним інформаційним вмістом можуть взаємодіяти між собою, використовуючи детально розроблені та впроваджені інтерфейси та протоколи [19].

3.3 Інформаційний сектор як сфера впливу Мінцифри

Компетенція та сферу впливу новітнього Міністерства цифрової трансформації було розширено, коли 9 жовтня 2020 року Кабмін прийняв Постанову «Деякі питання об'єктів критичної інфраструктури» №1109. Документ закріпив наступні процедури, виконуючи частину другу Статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» [20]:

1) Порядок віднесення об'єктів до об'єктів критичної інфраструктури;
2) Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави (далі – Перелік);
3) Методика категоризації об'єктів критичної інфраструктури.

У постанові було закріплено значення необхідних термінів для забезпечення чіткого й повноцінного виконання перелічених вище процедур. Термін «сектор (підсектор) критичної інфраструктури» вживається у випадку, коли необхідно описати чи перелічити певний розгалужений комплекс КВОІ, що відносяться або до спільної галузі економіки, або подібні у функціональному призначенні. Це поєднання допоможе підсилити безпеку і стійкість таких об'єктів, оскільки буде враховуватися специфіка надання окремих життєво важливих функцій та/або послуг. Також одним із таких термінів виступає «уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури», що окреслює законодавчо закріплений центральний орган виконавчої влади або інший державний орган, який буде керівним у впровадженні державної політики у визначеним за ним сектором для своєчасного й надійного регулювання стану безпеки критичної інфраструктури [20].

У Переліку визначено 11 секторів КІ, і вони містять всього 18 підсекторів. Мінцифри встановлено уповноваженим органом державної влади, який відповідальний за інформаційний сектор КІ з двома підсекторами: інформаційні технології та телекомунікації. Надання відповідних послуг може поєднуватися на одному критично важливому об'єкті інфраструктури, або конкретний пункт буде притаманний лише унікальному такому об'єкту. На кожному такому КВОІ обов'язково працюють люди, і вони як частина SCADA впливають на стан захищеності таких об'єктів та забезпечення призначених сервісів, тому оператори – одна з цілей країни-противника для виведення з ладу всього КВОІ.

3.4 Єдиний портал державних послуг і мобільний застосунок «Дія»

На середину 2022 року можна сміливо заявити, що команда Міністерства цифрової трансформації України на чолі з Михайлом Федоровим успішно досягла вражаючих результатів на шляху до поставленої цілі – перевести 100% публічних послуг в онлайн, незважаючи на трудомісткі роботи, спричинені пандемією. Для цього було прийнято чимало важливих кроків.

6 лютого 2020 року Міністерством цифрової трансформації було представлено мобільний додаток «Дія», який з небагатьма доступними послугами на той час, започаткував впровадження в повсякденне життя українців концепції «Держава в смартфоні». Україна надала можливість громадянам засвідчувати посвідчення водія та свідоцтво про реєстрацію транспортного засобу без паперових екземплярів – лише в цифровому форматі. Наша держава стала четвертою країною у Європі та десятою на міжнародній арені, де стали доступні такі функції для громадян. З офіційної презентації мобільного застосунка за участі Президента України Володимира Зеленського стало достовірно відомо, що цифрові документи володітимуть юридичною силою, аналогічною до фізичних [21].

На поточний момент ідентифікація користувачів можлива трьома способами: через BankID (для банків, які долучилися до співпраці з Мінцифрою), Приватбанку та NFC, використовуючи наявні біометричні документи. Функціонування додатку

(тобто відображення даних з реєстрів) доступне в онлайн й офлайн режимах. Також Мінцифри здобули підтримку мобільних операторів України, які зробили мобільний застосунок «Дія» вільним від стягнення коштів.

Уже в застосунку користувач може отримати доступ до таких цифрових документів, якщо вони попередньо оформлені (типи цифрових документів, які вже додані поступово до двох попередніх): ID-картка (паспорти у формі книжки не будуть відображатися в «Дії»), паспорт громадянина України для виїзду за кордон, реєстраційний номер облікової картки платника податків, свідоцтво про народження дитини (доступний тільки для батьків), довідка внутрішньо переміщеної особи, студентський квиток.

Єдиний державний вебпортал електронних послуг (далі – Портал Дія) був ініційований задля того, аби забезпечити право кожного українця на доступ до електронних послуг у віртуальному форматі, і це стало можливим 2 квітня 2020 року. Офіційно визначений для цього ресурс – diia.gov.ua, і шляхом розробки цієї платформи українські ресурси будуть позбавлені дублювання сервісів, незручних процедур, однакових зон відповідальності та віджилих і пройдених інтерфейсів у минулому. Пріоритет роботи був направлений на те, аби цілодобово кожен охочий міг замовити державну послугу впродовж декількох хвилин, не витрачаючи час на черги та надмірні бюрократичні процеси. Шляхом входу до особистого кабінету тут реалізується доступ до відомостей, які зберігаються в реєстрах.

Для замовлення послуги на Порталі Дія необхідно авторизуватися, що підтвердити особу. Це можливо за допомогою системи ID.GOV.UA (Інтегрованої системи електронної ідентифікації), мобільного застосунку Дія (у разі наявності Дія.Підпис) або особистого ключа (файлового чи апаратного).

Реєстр адміністративних послуг (на Порталі Дія зазначено як «Гід з державних послуг») – це онлайн-репозиторій, розміщений за посиланням guide.diia.gov.ua, призначений для допомоги громадян з наданням точної та актуальної інформації щодо кожної державної послуги із зазначенням умов, строків, суб’єктів її забезпечення, органів, до яких оскаржується, нормативної бази, пов’язаних послуг тощо. Цей реєстр є частиною цілісного Порталу Дія і містить понад 1500

адмінпослуг, які згруповані в 17 категорій, кожна з яких представляє певну сферу діяльності, або додатково можна скористатися в інтерфейсі розподілом за 36 життєвими подіями.

З моменту поширення на території України пандемії коронавірусної хвороби у зв'язку зі збудником SARS-CoV-2 керівництво Мінцифри не залишилося осторонь від труднощів, з якими стикнулися українці в умовах ізоляції та роботи в дистанційному форматі. Від моменту виявлення першого випадку 3 березня 2020 року Михайло Федоров запровадив політику, спрямовану на захист громадян без потреби відокремлення від світу, через додавання додаткових функцій на Порталі Дія та в мобільному додатку.

Неоціненним внеском також вважаються зусилля Михайла Федорова та всієї команди Мінцифри загалом після початку повномасштабного вторгнення російських військ 24 лютого 2022 року. Оскільки приблизно 17,5 мільйонів українців користуються мобільним додатком «Дія» та Порталом Дія, то ці платформи використані для надання допомоги нашим громадянам та співпраці з державними органами з метою відбиття нападу. У рамках цього за три місяці війни команда Мінцифри запустила в додатку «Дія»: функцію швидкої допомоги армії шляхом переказу коштів; одержання одноразових виплат для тих, хто проживає на території бойових дій; трансляцію національних телеканалів; спеціальний «єДокумент» з юридичною силою на період воєнного стану; радіомовлення «Дія.TV»; відправку заявки про зруйноване або пошкоджене майно внаслідок воєнних подій для отримання компенсації; гру «єБайрактар»; послугу для підтвердження статусу внутрішньо переміщених осіб й одержання відповідних виплат (також доступно на Порталі Дія); оформлення статусу безробітного й одержання відповідних виплат (також доступно на Порталі Дія); проведення опитувань для вирішення пов'язаних з війною питань. На Порталі Дія також додано послугу «єДекларація» та подачу заявки на отримання грантів постраждалим бізнесом.

Разом із іншими небайдужими командами та представництвами Мінцифри реалізували: ІТ-армію та Інтернет Війська України, чатботи «Турботник» і «єВорог»

у «Telegram»; Telegram-канал і додаток «Повітряна тривога»; портал «єДопомога»; сайт «Доказ» із збором підтверджень злочинів російських військових; платформу «Truth Fund» для координації дій на інформаційному фронті; створення NFT-музею війни для збору коштів на потреби армії; платформу для сприяння релокацію бізнесу з небезпечних місць; мобільний додаток «Lepta».

Команда Мінцифри продемонструвала оперативне вирішення сьогоднішніх викликів шляхом розробки технічних нововведень для найбільш необхідних послуг українцям, таким чином, Україна впевнено розвивається та прямує до інтеграції з цифровим простором Європейського Союзу. Цифровізація не тільки запланованих сервісів, але й виникаючих у режимі реального часу пройшла успішно й допомогла українцям витрачати лише лічені хвилини на комфортне та безпечне віртуальне життя.

3.5 Формування реєстру критично важливих об’єктів інфраструктури інформаційного сектору

15 червня 2022 року введено в дію Закон України «Про критичну інфраструктуру» – вкрай важливий документ для закріплення державної політики у процесі побудови національного комплексу захисту КВОІ. У ньому надано деталізацію функцій та послуг, що характеризуються як фундаментальні для національних інтересів, оскільки результатом їх порушення стануть негативні наслідки для національної безпеки України. Таким чином, відповідальність Міністерства цифрової трансформації України, враховуючи проаналізований інформаційний сектор критичної інфраструктури, цілком реально буде направлений на наступні функцій та послуги із вище згаданого закону [22]:

1) урядування та надання найважливіших публічних (адміністративних) послуг;
2) інформаційні послуги;
3) електронні комунікації.

Закон передбачає створення реєстру критично важливих об’єктів інфраструктури (далі – Реєстр), що являтиме собою автоматизовану систему з реалізацією особливих вимог щодо її експлуатації. Відомості в Реєстрі будуть відкритою інформацією, для безкоштовного та загального доступу громадян з будь-якої точки світу, окрім інформації з обмеженим доступом. Також зазначено, що до таких даних буде організовано цілодобовий доступ на офіційному веб-сайті [22].

У законі надано перелік критеріїв, за яким в Україні будуть визначатися КВОІ. Такі вимоги необхідні, аби точно відобразити значущість віднесених об’єктів серед екологічної, економічної, політичної чи соціальної складової українського суспільства.

Дотримання критеріїв і об’єктивна оцінка кандидату до Реєстру стане головним чинником у всіх процедурах забезпечення безпеки співробітників, оборони установи, контролю правопорядку та подолання інцидентів, про які невідкладно мають сповіщати оператори критично важливих об’єктів інфраструктури до відповідного управління Національної поліції України, СБУ, підрозділів Національної гвардії України та інших державних установ для усунення проблем з фізичною та кібербезпекою. Обов’язковим є також сповіщення Служби безпеки України про підозру та ознаки потенційних диверсій, терористичних актів, актів кібертероризму, направлені на системи КВОІ [22].

Загалом можна теоретично припустити, враховуючи викладені в [22] критерії та вимоги, які установи, задіяні в діяльності Міністерства цифрової трансформації України, будуть в найближчому майбутньому віднесені до Реєстру.

Міністерство цифрової трансформації розміщується в столиці за адресою вулиця Грушевського 12/2 – будівля Кабінету Міністрів України. Це одна із складових урядового кварталу Києва – району у середмісті міста, охоплений вулицями Грушевського, Інститутською та Банковою, де розташовані вищі державні органи влади, серед яких також Офіс Президента України, Верховна Рада України та певна сукупність депутатських комітетів.

Підпорядкованим органом (або підвідомчим органом, тобто таким, яким визначено нищим за рівнем у стані організаційних відносин) Міністерства цифрової

трансформації визначено Адміністрацію Держспецзв'язку [23], розміщену за адресою місто Київ, вулиця Солом'янська, будинок 13. Установа має спеціальний статус у системі центральних органів виконавчої влади. Мета створення Адміністрації Держспецзв'язку полягає в забезпеченні й технічній підтримці спеціального зв'язку, виконання вимог щодо захисту інформації, організації заходів із кіберзахисту телекомунікацій та регулювання особливостей застосування радіочастотного ресурсу України.

Діяльність Мінцифри не обмежується лише регулюючими установами, оскільки їхня робота сконцентрована на функціонуванні високонадійного серверного обладнання, супутніх мережевих пристроїв та засобів для їх захисту та зберігання, які і забезпечують роботу сервісів для громадян. Такі потужності розміщують у центрах обробки даних і, таким чином, забезпечують безперервну роботу бізнес-процесів шляхом постійного електроживлення, швидкого реагування на неочікувані інциденти, підтримання необхідних кліматичних умов та стійкого з'єднанням з мережею.

De Novo – це лідер серед вітчизняних постачальників хмарних сервісів Infrastructure as a Service (далі – IaaS) і центрів обробки даних, інформаційна безпека якого сертифікована згідно з міжнародним стандартом ISO/IEC 27001:2013, а його операційні системи мають підтверджений висновок німецької компанії з виробництва програмного забезпечення SAP SE в розділі сервісів Cloud and Infrastructure Operations. Крім того, De Novo здобула атестати відповідності комплексної системи захисту інформації (далі – КСЗІ) інформаційно-телекомунікаційної системи «Розподілена платформа хмарних обчислень для надання послуг публічної, колективної та приватної хмари, за моделями «інфраструктура як сервіс» (IaaS) та «платформа як сервіс» (PaaS)» від Держспецзв'язку, тобто реалізований захист інформації відповідно до вимог нормативних документів із технічного захисту інформації [24].

Саме цей провайдер в Україні організував ЦОД рівня надійності Tier III та відповідно до вимог Національного банку України. Це міжнародний показник власне того, наскільки надійними є ЦОД, а отже, захищені дані. Частка вітчизняного

ринку досягає 25%, і сьогодні серед клієнтів ЦОДу De Novo є найбільші банки України, оскільки саме ця компанія володіє платформою розміщення найбільшої IaaS хмари в державі. Розміщується у київському бізнес-центрі «Сирецька Роща» за вулицею Північно-Сирецька, будинок 1-3 [24].

GigaCloud – це українська IT-компанія, яка забезпечує послуги IaaS та Platform as a Service, тобто також, як і De Novo, надає майданчик для розвитку бізнесу. Серед клієнтів налічуються юридичні особи різних масштабів, а загалом 1300 представників з шести країн світу [25].

Компанія у 2016 році першою серед вітчизняних провайдерів підтвердила відповідність міжнародному сертифікату ISO/IEC 27001:2013, а в 2018 році також отримала атестат відповідності КСЗІ від Державної служби спеціального зв'язку та захисту інформації України. У 2021 році GigaCloud пройшла сертифікацію за стандартом безпеки даних індустрії платіжних карток Payment Card Industry Data Security Standard і, таким чином, стала першим провайдером хмарних технологій в Україні з такою відзнакою. В Україні GigaCloud розміщує власні потужності у двох дата-центрах в місті Києві: GigaCenter за вулицею Васильківська, будинок 37Б та BeMobile за вулицею Куренівська, будинок 21-А. Налаштована інфраструктура відповідає також рівню надійності Tier III [25].

Враховуючи потенціал компаній De Novo та GigaCloud, є закономірним той факт, що саме на їх базі розміщуються потужності Порталу Дія і мобільного додатку «Дія». Таким чином, ЦОДи двох провайдерів також можуть стати реальними кандидатами до реєстру критично важливих об'єктів інфраструктури [26].

Отже, проаналізувавши існуючі фронти діяльності Міністерства цифрової трансформації України, хочу зазначити, що воно має великий вплив на всі державні органи та провідні галузі держави, оскільки контролює діджиталізацію повсякденного життя українців та скупчує навколо себе інтелектуальний простір разом із ідеями, інвестиціями та кваліфікованими кадрами. Така рушійна сила українського розвитку повинна мати потужний захист усіх складових, починаючи із консолідації головних точок концентрації ресурсів в єдиному реєстрі критично важливих об'єктів інфраструктури.

РОЗДІЛ 4
РОЗРОБКА КОМПЛЕКСУ ЗАХОДІВ ЗАХИСТУ ВІД КІБЕРВПЛИВУ НА ПЕРСОНАЛ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

4.1 Ідентифікація кібервпливу

Кібервплив не можна сприймати як хаотичне, ненадійне та малозначне заняття, оскільки це злагоджена техніка використання вразливостей опрацювання й сприйняття інформації людським розумом, тобто віртуальна форма жорсткої і насиченої пропаганди. Уряди беруть участь у таємних онлайн-операціях, які мають на меті вторгнення, обман і контроль за допомогою поширення неправдивої інформації та використання хитромудрих суспільствознавчих тактик. У моделі Лімби, Плети, Агафонова і Дамкуса сектор культури безпеки відводиться якраз для роз'яснення персоналу необхідності дотримання всіх заходів безпеки, а також для відстеження та перевірки працівників на встановлені контролі.

Для виявлення операцій кібервпливу треба проаналізувати величезну кількість джерел інформації, представлених у різних формах. Поки технології штучного інтелекту вдосконалюються, аби бути корисними в кібервійні в аспекті підтвердження достовірності даних, офіцери з безпеки повинні власними силами й наявними інструментами зупиняти такі цифрові маніпуляції.

У контексті подібності до характеру впливу синонімами пропаганди виступають дезінформація, перекручування даних, обман, маніпуляція, контроль над розумом та його замилювання. Пропаганда в загальному розумінні означає поширення або просування окремих ідей. Кібертехнології ідеально підходять для виконання такого завдання, оскільки з доступом до Інтернету всіх охочих пропаганда має змогу блискавично розповсюджуватися. Важливим принципом пропаганди є розкрутка або управління новинами, що передбачає їх корегування для мінімізації потоку негативної інформації та спроби максимізувати позитивний ефект необхідних відомостей серед публіки. На жаль, соціальні мережі, які нещодавно

сприймалися як платформа для розваг, обміну ідеями, пошуку натхнення, заробітку та спілкування, стали інструментом російського кібервпливу для дезорієнтації українців під час постійного надходження новин. Психологічна маніпуляція через онлайн-джерела інформації мала на меті здобути прихильність населення України, переманити їх на свою сторону та зробити своїх пособниками. Telegram, як один з широко використовуваних російськими політтехнологами месенджерів, сприяв розповсюдженню всіх можливих технік кібервпливу.

4.2 Використані техніки протягом кібервпливу

Головний сенс кібервпливу в тому, що ворожі політтехнологи зосереджуються не на тому, що сказано чи написано, а на тому, як це донесено до жертви. Пропаганда не дає однозначних відповідей. Коли населенню занадто прямо нав'язують чужу й контрастну точку зору, воно чинить опір. Натомість пропаганда в соціальних мережах і месенджерах побудована таким чином, що люди починають сприймати події зовсім інакше – спотворено й без прив'язки до правдивого стану речей, – і вважають, що такі висновки зробили самостійно.

Виділимо наступні методи із прикладами, які застосовували ворожі політтехнологи протягом кібервійни лютого-травня 2022 року в соціальних мережах:

1) Поширення напівправди на офіційних ресурсах є зручною технікою для кібервоїнів опонента. Надання лише «зручної» інформації, без доказів, пояснень і деталей робить їх, по суті, безпечним джерелом новин, проте такий контент не розкриває глобальної ситуації і приховує найбільш важливі моменти. Пропагандисти враховують лінощі читачів, які в безперервному потоці не будуть звертатися до першоджерела. Приклад розповсюдження напівправди представлено на Рис. 4.1. Ресурс «РИА Новости» в Telegram від 4 березня не надає реальні причини зупинки бізнесу на російському ринку виробників-гігантів інформаційних технологій.

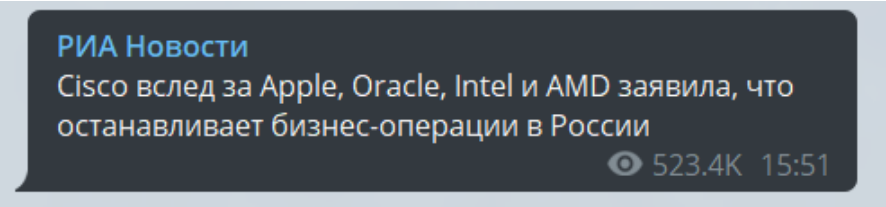

Рисунок 4.1 – Приклад №1 російського кібервпливу від 4 березня

У дописі вказується тільки підсумок із заяв компаній. Наприклад, в позиції фірми «Cisco» було наведено таке твердження: «Враховуючи ескалацію війни та на підтримку українського уряду та населення, ми в найближчому майбутньому припиняємо всі ділові операції, включаючи продажі та надання послуг у Росії та Білорусі».

2) Спотворення гучних фактів також активно використовується адміністраторами ворожих соціальних мереж. 3 квітня активно просувалася соціальними мережами чергова операція в кіберпросторі щодо проведення військових навчань польської армії з 1 травня. Тим часом, російські політтехнологи, а потім й опозиціонери, отримали шанс перекрутити дану інформацію у свою користь: нібито Польща планує напасти на Західну Україну, аби поділити з Росією області між собою. Через розгалужену мережу пропаганди це явне перекручування реальних подій опублікувало й британське видання Reuters, підтверджуючи заяву каналу «Грозный-Информ», яка представлена на Рис. 4.2.

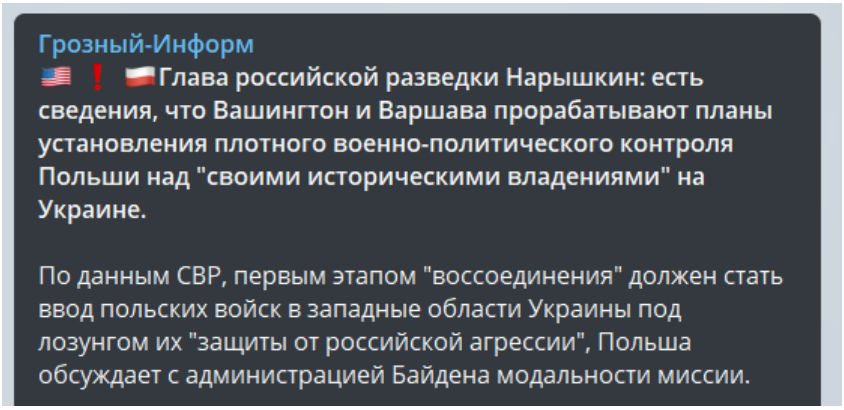

Рисунок 4.2 – Приклад №2 російського кібервпливу від 28 квітня

Польща не залишилася осторонь від такого спотворення фактів і, очікувано, заперечила сфальсифіковані заяви Голови Служби зовнішньої розвідки Росії.

3) Приклад виправдання й донесення раціоналізації існуючої ситуації представлено в дописі від 19 квітня на Рис. 4.3.

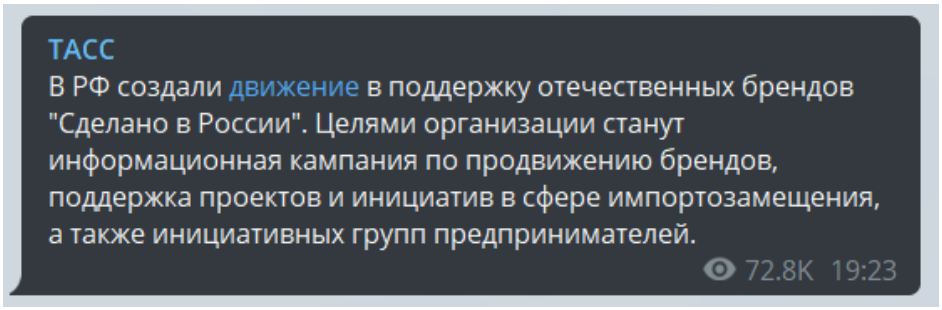

Рисунок 4.3 – Приклад №3 російського кібервпливу від 19 квітня

Як правило, використання таких заяв спрямовано на деморалізацію та спад бойового духу супротивника через докази, що його зусилля були даремними, та ще й виявилися корисними для держави під час кібервійни. Telegram-канал «ТАСС» поширив новину про те, що в рамках кампанії заміни продуктів імпорту міжнародних компаній, які відмовилися від російського ринку через вторгнення в Україну, буде надано підтримку вітчизняним виробництвам. Тобто відтік закордонних товарів ще й забезпечить можливість росіянам розвиватися самостійно та працювати на благо економіки країни.

Продовження цієї «патріотичної» ідеї було також оприлюднено у зверненні Дмитра Медведєва, заступника голови Ради Безпеки Російської Федерації, 26 квітня, де він наводить твердження (звичайно, без доказів), що ті ж самі компанії намагаються повернутися до «перспективного» російського ринку, Рис. 4.4.

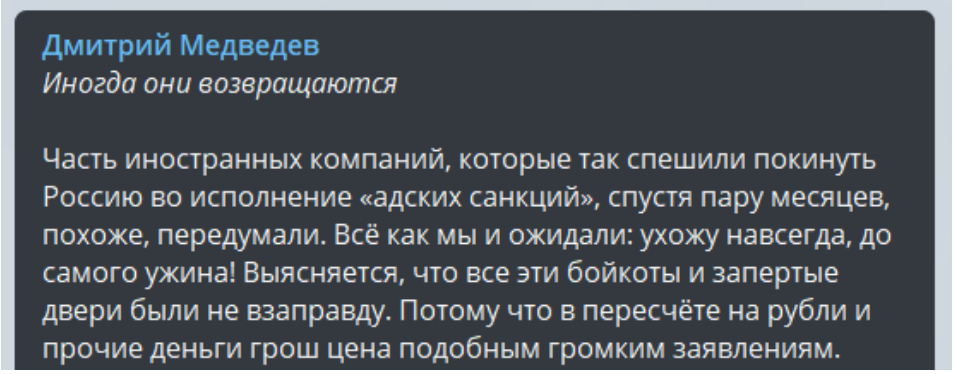

Рисунок 4.4 – Приклад №4 російського кібервпливу від 26 квітня

Загалом, подібними висловлюваннями опонент приховує власні страхи, вразливості й немічність.

4) Брехня – це незамінний інструмент в арсеналі кіберпливу путінського режиму. Від 1 травня 2022 на офіційному ресурсі Російської Федерації «РИА Новости» було розміщено допис, представлений на Рис. 4.5, що містить повністю брехливу інформацію.

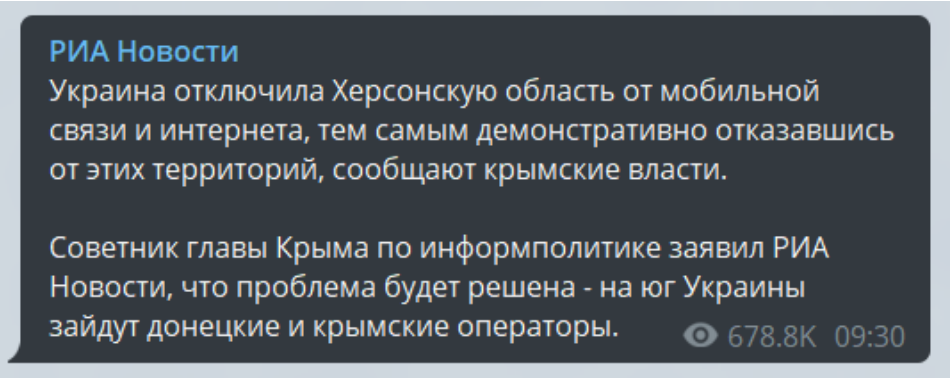

Рисунок 4.5 – Приклад №5 російського кібервпливу від 1 травня

Цього ж дня Держспецзв'язку опублікувала дані про те, що відбувалося насправді: чому і яким чином відбулося відключення ворожими підрозділами зв'язку та Інтернету в окупованих областях.

Також однією із найбільш абсурдних «новин» російської сторони, яку досі просувають у всіх можливих джерелах, стали секретні дані розвідки про розміщення на території України біолабораторій. Ця брехня просувалася в кіберпросторі задовго до початку повномасштабного вторгнення, але після 24 лютого майже кожного дня публікувалися фейкові новини на цю тему, приклади яких наведено на Рис. 4.6-4.9 від каналу «IZ.RU».

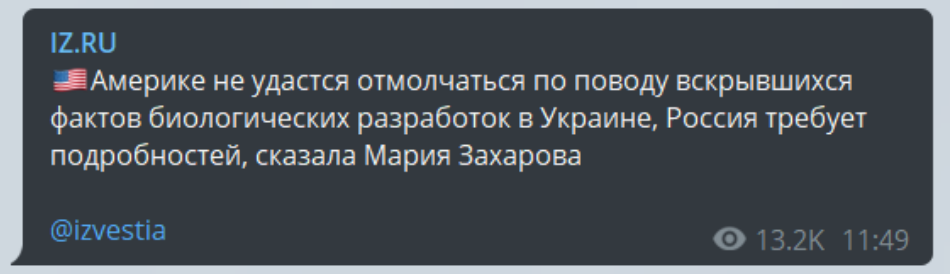

Рисунок 4.6 – Приклад №6 російського кібервпливу від 9 березня

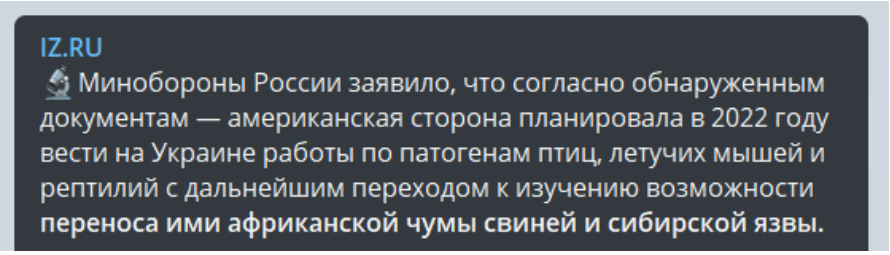

Рисунок 4.7 – Приклад №7 російського кібервпливу від 10 березня

Рисунок 4.8 – Приклад №8 російського кібервпливу від 24 березня

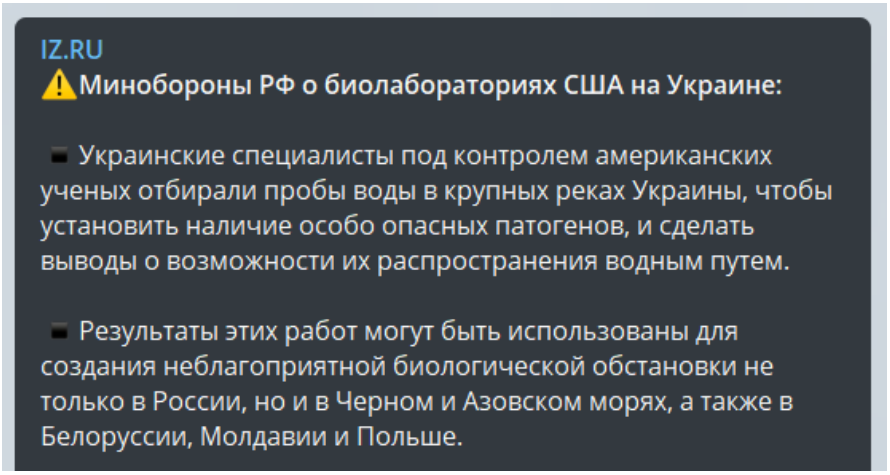

Рисунок 4.9 – Приклад №9 російського кібервпливу від 14 квітня

Таким чином, російські політтехнологи довели, що поширювати брехню набагато безпечніше й надійніше, аніж правду й визнання своєї поразки.

5) Використання аргументів, які націлені безпосередньо на особистість опонента, а не на його кроки, заяви чи рішення, стало незамінною технікою пропаганди. Відповідною інформацією проводиться дискредитація супротивника в кіберпросторі, аби його прибічники перейшли на протилежну сторону.

Російський кібервплив обрав дуже ганебний спосіб «отруєння джерела» шляхом нападів на Володимира Зеленського. Офіційні Telegram-канали розповсюджували ганебні наклепи на Президента України, вдаючись до вигаданих доказів. До таких брудних дій вдаються не тільки анонімні адміністратори, але й обличчя держави, як наприклад зробив Сергій Лавров, Міністр закордонних справ Росії, в інтерв'ю від 19 квітня, фрагмент якого представлено на Рис. 4.10.

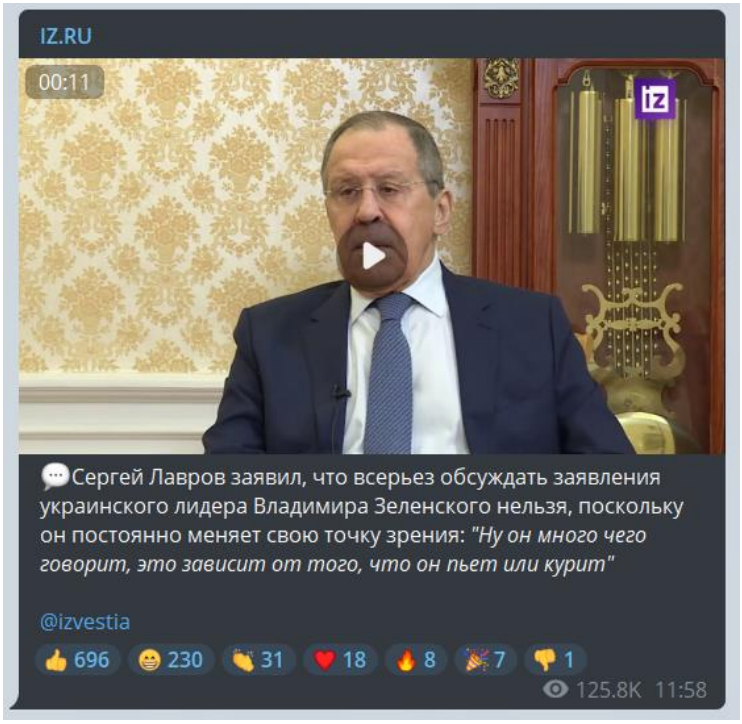

Рисунок 4.10 – Приклад №10 російського кібервпливу від 19 квітня

Приклади інших ганебних атак у кібепротистоянні наведено на Рис. 4.11-4.13.

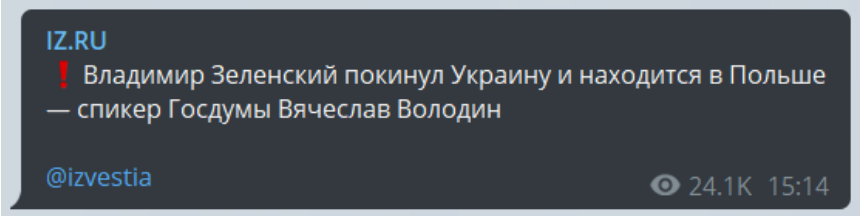

Рисунок 4.11 – Приклад №11 російського кібервпливу від 4 березня

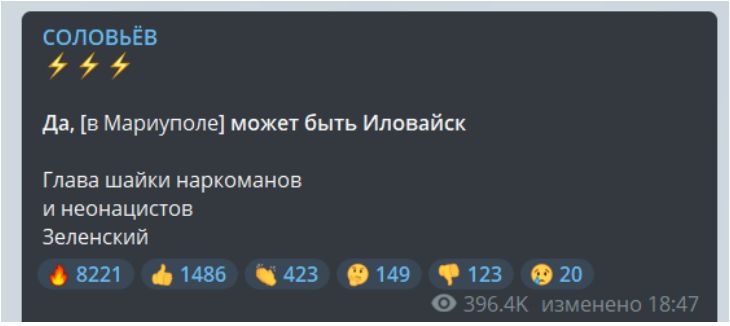

Рисунок 4.12 – Приклад №12 російського кібервпливу від 16 квітня

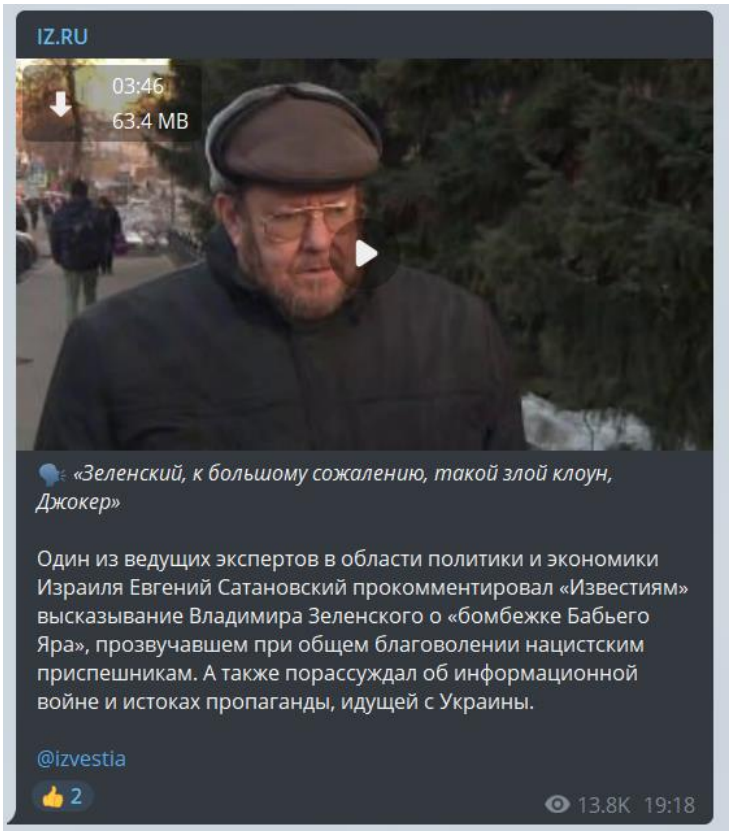

Рисунок 4.13 – Приклад №13 російського кібервпливу від 2 березня

Залучення цього прийому у свій спектр пропаганди зайвий раз демонструє, що російські джерела інформації, навіть офіційні, побудовані на зомбуванні читачів.

6) Багатократне повторювання використовується політтехнологами, аби схилити читачів до віри в конкретну ідею через її надмірну кількість у потоці інформації. Одноманітний й докучливий контент починають сприймати як той, що справді відповідає дійсності, і така маніпуляція людським розумом у довгостроковій перспективі породжує послідовників. Завдяки повтору тих самих даних за періодичні проміжки часу кібервоїни опонента нав’язували безглузді твердження

без жодних обґрунтувань чи пояснень. Так сталося і на каналі «РИА Новости», де протягом більше двох місяців поширювали фейкові новини, ніби Маріуполю залишилося декілька годин до захоплення російськими бойовиками, але їхні очікування не справджувалися, що підтверджує повторення аналогічних заяв через деякий час згідно з Рис. 4.14-4.18.

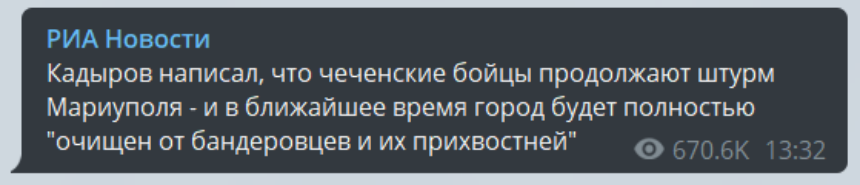

Рисунок 4.14 – Приклад №14 російського кібервпливу від 17 березня

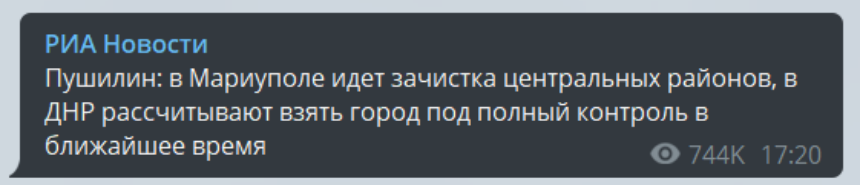

Рисунок 4.15 – Приклад №15 російського кібервпливу від 28 березня

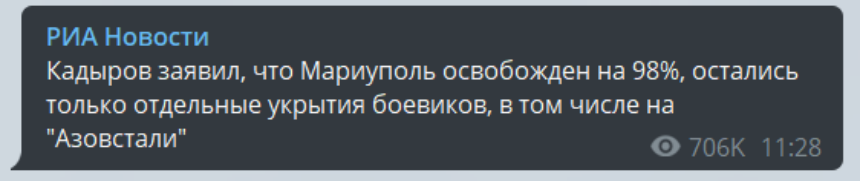

Рисунок 4.16 – Приклад №16 російського кібервпливу від 8 квітня

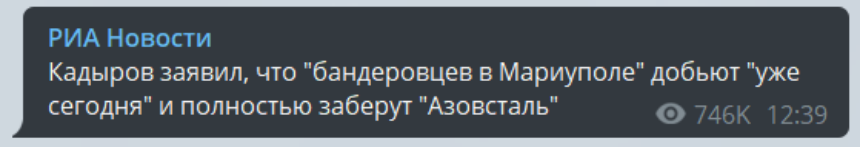

Рисунок 4.17 – Приклад №17 російського кібервпливу від 19 квітня

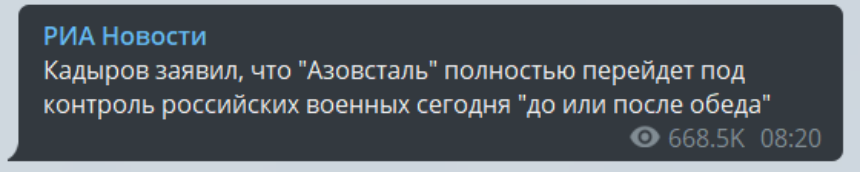

Рисунок 4.18 – Приклад №18 російського кібервпливу від 21 квітня

Російські військові фігури повторювали одне й те саме, кожного разу додаючи більшої переконливості своїм заявам. Центр протидії дезінформації при РНБО України (далі – ЦПД) попередив і застеріг українців про цей спосіб кібервпливу.

7) Залякування – необхідний засіб кібервпливу для провокування розгубленості й збентеження серед звичайних громадян, що вимикає в них критичне мислення. Шляхом апелювання до страху російські ЗМІ, використовуючи прямі заяви Лавров, поширювали прямий ядерний шантаж і погрозу розгортання Третьої світової війни, як це зробило видання «360tv» 25 квітня, допис якого представлено на Рис. 4.19.

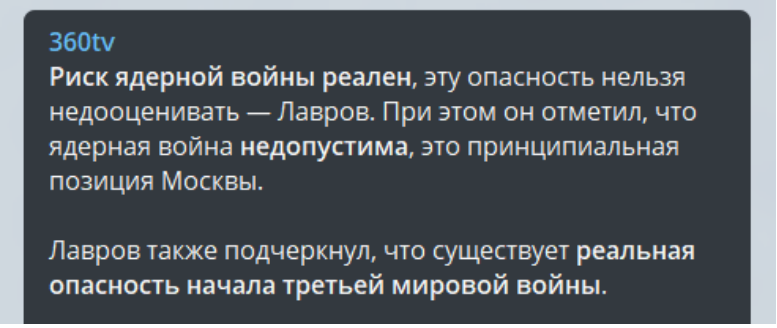

Рисунок 4.19 – Приклад №19 російського кібервпливу від 25 квітня

8) Залучення до пропаганди в кіберпросторі красивих, успішних і щасливих людей виконує важливу роль у поширенні вигаданої інформації. Як правило, представники шоу-бізнесу, спорту чи культури, а також блогери (у наш час їх всюдисущності на різних соціальних платформах) домагають владі, частіше за все за контрактом з отриманням грошової винагороди. Оскільки такі особистості мають певний успіх у своєму житті, наслідування поширюваних ними позиції та ідей може здатися читачам як крок до власного процвітання. Тим паче, більшість відомих людей сприймаються як гарант достовірності, бо вони самостійно побудували кар'єру з нуля, тобто розуміють хід думок звичайних громадян.

До лав пропагандистів ворога приєдналися не тільки корінні росіяни, але й митці українського походження. Усі вони, звертаючись до своїх підписників і публікуючи проплачену підтримку путінського режиму, допомагають йому в кібервійні. Наприклад, допис в Instagram російського виконавця Станіслава

Михайлова від 4 березня направлений на виправдання дій своєї держави і заклик до згуртованості співвітчизників, Рис. 4.20.

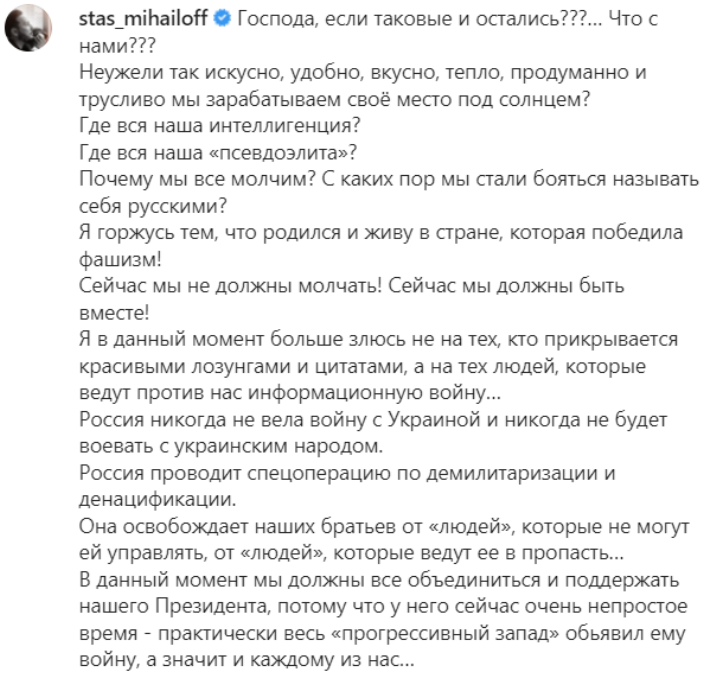

Рисунок 4.20 – Приклад №20 російського кібервпливу від 4 березня

9) Звернення до почуттів і переживань великих народних мас також допомагає російським політтехнологам досягати цілей кібервійни. Даний інструмент позбавляє необхідності взагалі надавати певні докази чи пояснення, а натомість спекулює упередженнями та переконаннями через емоційно насичені повідомлення. Виклик позитивних чи негативних почуттів таким чином є засобом замилювання раціональних тверджень, або заміна їх відсутності.

Особливо апеляція до жалості, несправедливості та безкарності, яка простежується в конкретних повідомленнях, слугує стимулом для залучення більшої кількості послідовників. Даним способом активно користуються російські пропагандистські ресурси, аби просувати власні абсурдні ідеї.

Наприклад, канал «IZ.RU» демонструє 5 травня шляхом поширення відео, як окупанти опікуються тваринами на захоплених територіях України, і наголошують на тому, що без їхнього вкладу в забезпечення необхідних умов існування дельфіни б тяжко хворіли. Об’єднавши в одному дописі, представленому на Рис. 4.21, і жаліть до морських істот, і прогрес окупованого Криму, і просування ідеї «росіяни-

миротворці» та «росіяни-визволителі», адміністратори каналу розвивають прихильність до нової влади у читачів.

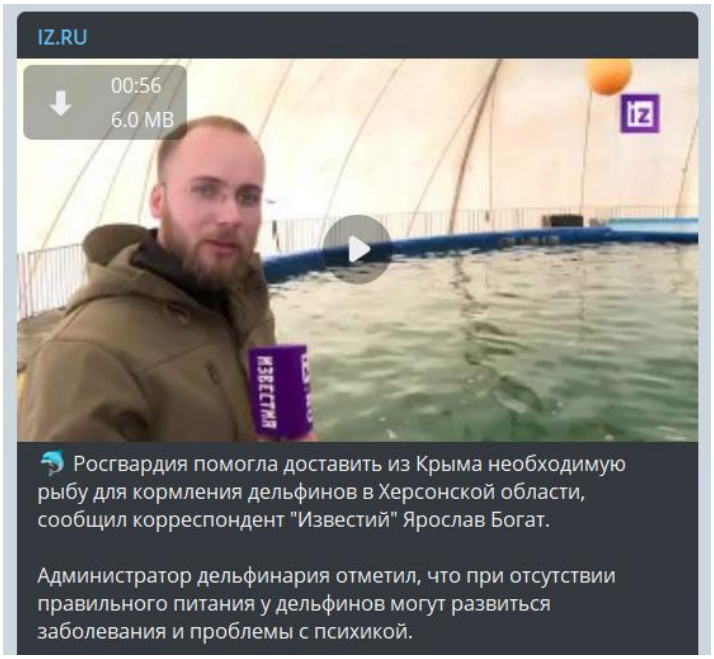

Рисунок 4.21 – Приклад №21 російського кібервпливу від 5 травня

10) Контент, де головні ролі надані простим людям, – легка й поширена пропаганда російських ЗМІ, оскільки такі відеорепортажі та фото вони виготовляють із залученням акторів. Матеріальна підтримка, співпереживання горю, вирішення нагальних проблем і задоволення базових потреб стали актуальним матеріалом, аби привернути увагу до світлих і мирних намірів окупантів. Головна суть – показати, що російська влада розуміє звичайних громадян і стає на їхню сторону. Якщо сценарій побудований із представником загарбників (журналіст, ведучий, мер, командир тощо), у діалозі з цивільним він спілкується жаргонізмами чи діалектом, аби показати, що максимально наближений до цієї людини.

Від 29 квітня Telegram-канали пропагандистів розповсюджували відео з нібито налагодженим ритмом життя людей в окупованому на той час Бердянську. У даному ракурсі російські загарбники уособлювали «рятівників» і «миротворців». Повідомлення власне спрямоване на здобуття підтримки від звичайних громадян шляхом демонстрації щастя й радості від таких самих людей. Росіяни ніби передають приховане послання у відеоролику: «Ми хороші, подивіться, як багато робимо для вас». Окупанти жертовно несуть мир у місто та позбавляють його від

наслідків розгромів. Кібервплив загалом був направлений на південні міста й селища, вільні від росіян, аби переманити їх на свою сторону. Відео і текст ворожого допису з каналу «Readovka» представлений на Рис. 4.22.

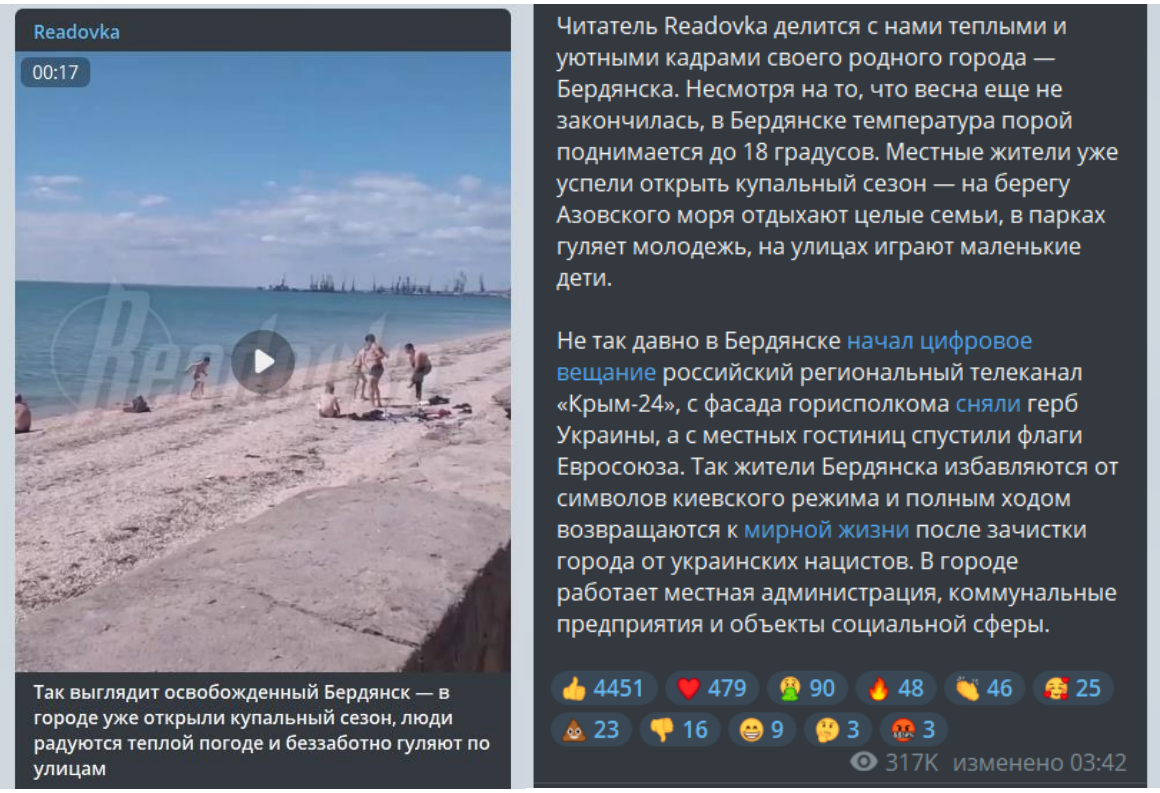

Рисунок 4.22 – Приклад №22 російської пропаганди від 29 квітня

ЦПД застеріг громадян України, що така психологічна тактика є потужним нападом у настільки критичній ситуації. Даний контент відображає лише вправні, хоча й неякісні, цифрові ілюзії із залученням акторів з метою звернення до цивільних.

11) «Махання прапорами» – техніка, що передбачає розповсюдження патріотичних настроїв під час кібервійни. Використання державних прапорів, військової символіки й традиційних пісень, звернення до історичної спадщини, культ діячів минулого – спосіб заявити про свою силу й згуртованість, а тому – морально подавити жертву й виграти бій фактично без його проведення.

Серед проявів такого штучного патріотизму виділявся мотивуючий контент з акцентом на незламність і перемогу. Російські політтехнологи спонсорували медійних діячів, аби ті поширювали наперед підготовлені дописи чи відеозвернення.

Подібний контент для поширення в мережі з винагородою представлено на Рис. 4.23, де прояв піднесених патріотичних почуттів оцінюється в один стік кави.

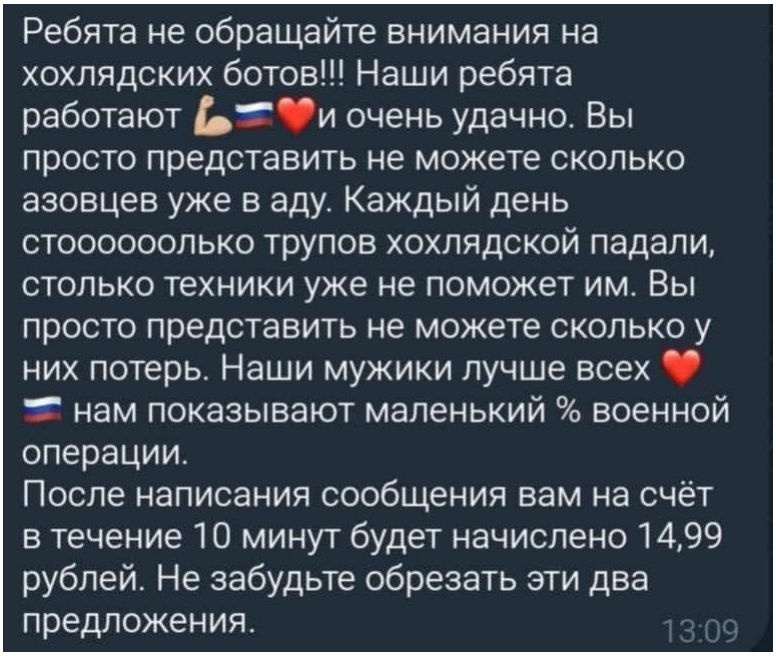

Рисунок 4.23 – Приклад №23 російської пропаганди

Відповідні схеми кібервпливу є примітивними, проте здатні знесилити читачів шляхом агресивної реакції та концентрації уваги на спам-повідомленнях, а не на достовірних даних від офіційних ресурсів.

12) Маніпуляція фактами – найбільш витончена техніка кібервпливу, оскільки від російських редакторів навіть не вимагається щось вигадувати, а лише трактувати офіційну інформацію так, як це їм вигідно. Підлаштування певного факту до необхідного курсу пропаганди виявляється неабияк ефективно в стані кібервійни, адже такий контент у соціальних мережах може подаватися та сприйматися як гіпотетичний, потенційний або єдиний раціональний висновок з усіх імовірних.

На Рис. 4.24 представлений допис, який російська пропаганда просувала 25 квітня у ЗМІ під гучним заголовком «Австрійці підтримали слова глави МЗС країни щодо членства України в ЄС». Жорстке узагальнення позиції громадян Австрії зробило цю новину сенсаційною, хоча не можна заперечувати припущення, що російські редактори спиралися лише на коментарі та вираження поглядів від проросійських представників держави або діаспору. Таким чином, маніпуляція інформацією не має підстав для її розгляду як достовірної.

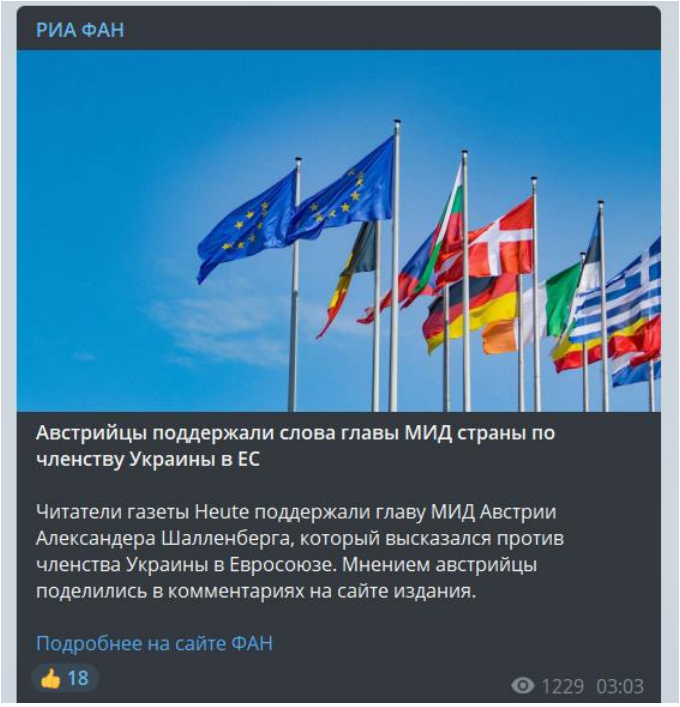

Рисунок 4.24 – Приклад №24 російської пропаганди від 25 квітня

ЦПД спростував таку заяву відзначивши, що висловлення коментаторів не може відображати ставлення більшості громадян Австрії до України, а також надав офіційну статистику щодо соціологічних опитувань серед країн Європи.

13) Обвинувачення у розповсюдженні фейкової інформації – спроба контрнаступу російських технологів з кібервпливу з метою прищеплення недовіри українців до вітчизняних ЗМІ. Насправді фотошоп чи монтаж відео з перевдяганням акторів разом із грамотно складеною легендою, або дані секретної розвідки, наприклад, можуть здійснити резонансні перетворення у світобаченні громадян супротивної держави. Розвінчувати фейки та переконувати в протилежному в кіберпросторі – надважке завдання з точки зору сприйняття людини.

Росіяни не залишали спроби ввести в обману українців, проте в більшості випадків через неякісне виконання технічних завдань з пропаганди вони демонстрували провальні матеріали в соціальних мережах. Прикладом хочу навести досить викривальний допис від пропагандистського каналу «Sputnik Ближнее зарубежье», яке наголосило, що в Україні «повторно» загинув американський активіст Берні Горес, хоча насправді роком раніше вже було оголошено про його смерть від рук талібів. Було прикріплено два дописи з однаковим фото, Рис. 4.25.

Рисунок 4.25 – Приклад №25 російської пропаганди від 27 лютого

Насправді тут дуже легко розібратися: обидва акаунти в Twitter є непідтвердженими (немає синьої галочки), що є неприпустимо для такої провідної агенції, як CNN, Cable News Network, отже їх не можна сприймати як достовірні джерела інформації. Використовуючи ресурс TinEye для реверсивного пошуку фото можна дізнатися, що на фото насправді зображений Джорді Джордан, особа, яка ніяк не пов'язана з обома ситуаціями. Отже, фейк окупантів розкрито, як і тривіальну спробу вплинути на ситуацію в кіберпросторі України.

З огляду на вищевикладені приклади можна зробити висновок, що відколи Росія вторглася в Україну, то війна перестала бути схожою на всі попередні, оскільки українці мали мобільні телефони та доступ до соціальних мереж. На українському кіберфронті зусилля з пропаганди не досягли успіху, тому громадяни України змогли побачити істину крізь туман війни. Кібервійна перевела на новий етап взаємодію між старими та новими медіа – численними потоками даних, які йдуть від Twitter до телебачення й радіо, TikTok і Telegram і в зворотному напрямку.

Таким чином, у першій у світі кібервійні українці відійшли від відносно статичної комунікаційної моделі, коли журналісти повідомляють про новини в рамках заздалегідь визначених обмежень і форматів, до інтенсивної фрагментації і навіть участі.

Оскільки кібервійна є ключовим компонентом нинішньої війни, то вона має відношення до всіх українських Інтернет-сервісів і особливо до критично важливих об'єктів інфраструктури, які їх підтримують. Дестабілізація вітчизняних онлайн-ресурсів можлива не лише через технічний спосіб виведення з ладу або порушення нормального функціонування, а й шляхом засобів кібервпливу на персонал, що залучений до обслуговування такої інфраструктури. Російська влада на це досі розраховує, тому операторів КВОІ у першу чергу необхідно убезпечити від пропаганди з боку агресора.

Усі офіційні ресурси Росії в соціальних мережах транслюють лише свою версію подій: ніякої війни їхня країна не веде, лише спецоперація. Уряд окупантів зосередився на безпрецедентній кампанії дезінформації, у рамках якого соціальні мережі транслюють російських військових під час «визволення» Україну від неонацистів і наркоманів разом з розповідями аудиторії про те, що українці завдають собі всієї шкоди. Постановочні сцени підсилюють операції кібервпливу.

Спільнота Check Point Research (далі – CPR) проводить глибокі дослідження та розвідку, що стосуються загроз, аналізів і звітів із здійснених кібератак. Їхня діяльність спрямована на обмін розвідувальною інформацією, яка сприяє розкриттю потенційних ризиків у кіберпросторі і розвитку міжнародної співпраці в сфері кібербезпеки. Спільнота самостійно провела розслідування щодо використання Telegram у російсько-українській кібервійні, і з 24 лютого дослідники CPR виявили приблизно в шість разів більше груп у соціальній мережі, що стосуються протистояння, ніж за день до вторгнення. Telegram став цифровим авангардом конфлікту, де люди онлайн обирали сторону. 71% груп Telegram, які мали відношення до війни, розміщували новини з невідредагованою і часто неперевіреною інформацією. Найпопулярнішим типом каналів були ті, які

транслювали (або тільки прикривалися даною діяльністю) свіжу інформацію безпосередньо з лінії фронту.

Простеживши лише частину інформаційного потоку, можна підкреслити, що Telegram, як й інші онлайн-ресурси, став одночасно й опорою, і ворогом українців у кібервійні. Форми пропаганди активно розповсюджувалися через цей миттєвий месенджер, що призвело до масштабного кібервпливу на громадян України, проте боротьба із шкідливим трафіком від російських політтехнологів стала настільки потужною, що перетнула всі можливі кордони.

4.3 Комплекс заходів щодо захисту від кібервпливу

Під час кібервійни влада України всебічно підтримувала право на свободу думки і слова своїх громадян, закріпленого в Статті 34 Конституції України. Ця позиція української влади була підтверджена в Постанові Верховної Ради України №2190-IX «Про Заяву Верховної Ради України про цінність свободи слова, гарантії діяльності журналістів і засобів масової інформації під час дії воєнного стану» від 14 квітня 2022 року.

Кожен, хто був підключений до української мережі зв’язку, мав змогу через онлайн-платформи, у тому числі й Telegram, читати й знаходити будь-яку інформацію. Вважаючи на неминучий кібервплив з боку російських політтехнологів українські можновладці провели масштабні дії щодо захисту українців у віртуальному просторі. Такі вектори діяльності мали успіх і позитивно сприймалися громадянами нашої країни.

На момент написання цієї роботи багато даних щодо роботи українських політичних діячів залишилися неоприлюдненими, бо акти кібервійни, як і бойові дії, не припинилися. З метою недопущення розкриття оборонних тактик і способів ведення контрнаступу на цифровому фронті уряд відповідально тримає багато відомостей в таємниці. Натомість на фіксації і відстеженні ефективних векторів роботи влади увагу не зосереджено, хоча вони можуть стати незамінними інструментами захисту в майбутньому для будь-якої іншої держави. Ці обставини

зумовлюють необхідність у розробці комплексу заходів щодо захисту інформаційного сектору держави шляхом паралельного дослідження, аналізу та доопрацювання проведених Україною операцій у кіберпросторі, результати яких розміщені у відкритих джерелах та на офіційних сторінках представників влади в соціальних мережах. Зазначений комплекс буде розроблений враховуючи розгортання кібервійни разом із повномасштабним вторгненням на територію, тобто оборону від гібридної війни.

Необхідно зауважити, що формулювання «комплекс» в контексті забезпечення захисту від кібервпливу передбачає необхідний мінімум взаємодоповнюючих заходів, направлений на донесення персоналу КВОІ, а також населенню загалом, правдивої інформації та запобігання поширення ворожої пропаганди в межах компетенції відповідного органу. Захід розглядається як легальна скоординована діяльність у кіберпросторі, яка уособлює негайний захист під час кібервійни.

Комплекс заходів щодо захисту інформаційного сектору держави від кібервпливу під час кібервійни

I. Національні заходи

1. Організаційні

1.1 Впровадження офіційного органу, відповідального за спростування пропаганди (далі – ОВСП).

1.2 Впровадження офіційних онлайн-представництв у соціальних мережах з їх верифікацією для глави держави, ОВСП, вищих структур держави (далі – ВСД) – головних органів законодавчої, виконавчої та судової влади, силових органів (включно з органами спеціального призначення, відповідальних за державну безпеку), органів місцевого самоврядування, – а також їх очільників і речників.

1.3 Трансляція впевненості та незламності від глави держави, очільників і речників ОВСП та ВСД у зверненнях до населення.

1.4 Регулярне надання актуального стану подій від глави держави, ОВСП та ВСД у залежності від сфери своєї відповідальності.

1.5 Заборона на публічні конфлікти між органами влади та засудження їх дій з боку інших органів.

1.6 Заборона на публічні оцінки результатів військових дій і рішення воєначальників, їх прогнози, коментарі щодо логістичних ланцюгів і центрів забезпечення, неофіційні шляхи евакуації від осіб, які не є представниками влади.

1.7 Заборона на акредитацію ЗМІ, які заперечують, підтримують або виправдовують дії ворога.

1.8 Заборона політичних партій, метою створення яких була співпраця з країною-агресором.

1.9 Блокування національними інтернет-провайдерами ворожих доменів.

1.10 Блокування можливості телефонувати громадянам до абонентів мобільних операторів з країни-агресора та заборонити її громадянам підключатися до національних мереж.

1.11 Обмеження роботи або відключення національних реєстрів та електронних ресурсів, які містять інформацію з обмеженим доступом.

1.12 Закріплення на законодавчому рівні переліку об’єктів, які заборонено публікувати в соціальних мережах і ЗМІ та яку відповідальність понесуть порушники.

1.13 Ліквідація роботи ворожих телеканалів і національних телеканалів, які заперечують, підтримують або виправдовують дії ворога.

1.14 Створення шляхом співпраці з національними мобільними операторами системи оповіщення на базі технології Cell broadcast для оперативного інформування громадян з відповідним сигналом. Попередження про такий спосіб комунікації на офіційних акаунтах.

1.15 Впровадження супутникового Інтернету на всій території держави.

1.16 Впровадження національного роумінгу на всій території держави.

1.17 Впровадження єдиного транслювання новин у вигляді марафону національними телеканалами з сигналом через супутник.

1.18 Впровадження єдиного транслювання новин у вигляді марафону національними радіостанціями.

1.19 Надання дозволу державними радіомовниками для ретрансляції їхнього сигналу радіостанціями країни.

1.20 Впровадження онлайн-довідника з інструкціями щодо надзвичайних ситуацій, які можливі під час гібридної війни, з доступом через веб-сайт та чат-боти в месенджерах.

1.21 Відстеження та ліквідація розміщення на онлайн-картах підозрілих міток та неіснуючих об’єктів.

1.22 Відстеження та ліквідація фейкових сторінок офіційних представників та органів країни в соціальних мережах.

1.23 Впровадження чат-боту для надсилання громадянами відомостей про колаборантів ворога, які розповсюджують у соціальних мережах дезінформацію, фейки, пропаганду та інший контент на користь ворога.

1.24 Впровадження чат-боту для надсилання громадянами новин з метою їх перевірки на справжність.

1.25 Впровадження чат-боту для перегляду новин з офіційних джерел за ключовими словами для зменшення інформаційного навантаження на громадян.

1.26 Створення SMS-розсилки з повідомленням про наявність мін і вибухонебезпечних об’єктів на території, де знаходиться абонент, а також з інструкцією про план дій, у разі їх знаходження. Попередження про таку розсилку на офіційних акаунтах.

1.27 Введення спеціальних процедур для можливості активації нових SIM-карток лише громадянами країни.

1.28 Співпраця органів влади з приватними установами для допомоги їм у перевірці інформації та поширення лише правдивих новин.

1.29 Співпраця органів влади з керівництвом сервісів, які дозволяють автоматизувати дії в соціальних мережах стосовно ворожих ЗМІ та пропагандистів – подання скарг на них або їх дописи.

1.30 Співпраця з діючими в країні медіасервісами для надання безоплатного доступу до інформаційних ресурсів.

1.31 Впровадження кампаній з боротьби з дезінформацією органами влади з вищими навчальними закладами.

1.32 Впровадження на тимчасово окупованих територіях агенцій для донесення найбільш необхідної інформації.

1.33 Впровадження спеціального центру для сприяння іноземним ЗМІ поширювати правдиві відомості про події.

1.34 Впровадження телебачення, мобільного зв'язку та Інтернету до бомбосховищ.

2. Довідково-роз'яснювальні

2.1 Надання від ОВСП переліку офіційних онлайн-представництв глави держави, вищих структур держави, органів місцевого самоврядування, їх очільників і речників на різних платформах.

2.2 Заклик та роз'яснення від ОВСП щодо використання в соціальних мережах тільки верифікованих національних та міжнародно визнаних ЗМІ.

2.3 Надання від ОВСП переліку ворожих джерел розповсюдження пропаганди та роз'яснень щодо небезпеки їх використання.

2.4 Надання від ОВСП переліку колаборантів, державних зрадників та прихильників ворога серед офіційних та публічних осіб.

2.5 Надання від ОВСП роз'яснень, як відрізнити ворожий онлайн-ресурс інформації від надійного.

2.6 Попередження та роз'яснення від ОВСП щодо поширення ворожих діпфейків та реклами у ЗМІ, SMS-розсилок та фішингових листів на пошту.

2.7 Попередження та роз'яснення від ОВСП щодо небезпеки розголошення персональних даних і банківських реквізитів на ворожих ресурсах, або будь-яких підозрілих чи невідомих платформах. Надання інструкції на випадок, якщо людина стала жертвою у схемах з незаконною маніпуляцією вище зазначених даних.

2.8 Попередження та роз'яснення від ОВСП щодо мети й способу діяльності ботів у соціальних мережах.

2.9 Попередження та роз'яснення від ОВСП щодо небезпеки інформації про поразку та капітуляцію країни та неможливість такої новини.

2.10 Попередження та роз’яснення від ОВСП щодо способів ворожих ЗМІ та пропагандистів змусити зневіритися громадян країни-жертви у владі та військовому керівництві, часто використовуючи її національну символіку.

2.11 Попередження та роз’яснення від ОВСП про небезпеку астротурфінгу на ресурсах соціальних мережах.

2.12 Попередження та роз’яснення від ОВСП щодо мети використання нових термінів і символів в матеріалах і заявах пропагандистів.

2.13 Попередження та роз’яснення від ОВСП щодо небезпеки надмірної емоційності у повідомленнях і закликів до розповсюдження у дописах від невідомих і неперевірених джерел і користувачів.

2.14 Попередження та роз’яснення про необхідність відслідковування підключених пристроїв до облікового запису певної платформи.

2.15 Попередження громадян, що мобільні ігри можуть використовуватися ворогом для залучення дітей до протиправної та небезпечної діяльності.

2.16 Попередження громадян не розповсюджувати патріотичні фейки, оскільки це призводить до погіршення здатності сприймати офіційні новини та факти.

2.17 Попередження громадян про можливу компрометацію пристроїв близьких та необхідність перевірки їх за допомогою додаткового способу комунікації, голосових повідомлень або персоніфікованих запитань.

2.18 Попередження громадян про корегувальників вогню у соціальних мережах під виглядом добродіїв, надання їх прикладів та роз’яснень небезпеки щодо передачі їм заборонених відомостей.

2.19 Роз’яснення від ОВСП, що супутникові тарілки не загрожують безпеці громадян, а є однією з найбільш стабільних технологій отримання інформації, що доступна з будь-якої точки країни.

2.20 Роз’яснення від ОВСП щодо небезпеки поширення непідтвердженої інформації в соціальних мережах, а також поширення тієї інформації, яка може становити пряму загрозу здоров’ю чи життю.

2.21 Заклик від ОВСП ознайомлюватися з текстами нормативно-правових актів лише на офіційних джерелах, верифікованих у соціальних мережах онлайн-представництв глави держави, ОВСП, ВСД, їх очільників та ЗМІ.

2.22 Заклик та роз’яснення від ОВСП щодо отримання інформації про кількість жертв або втрат лише з офіційних джерел.

2.23 Заклик та роз’яснення від ОВСП щодо необхідності блокування ворожих ЗМІ та пропагандистів на власних ресурсах соціальних мереж.

2.24 Заклик та роз’яснення від ОВСП щодо необхідності оперативного видалення чат-ботів з державними установами та ресурсів з національними новинами на період захоплення території ворожими військами.

2.25 Заклик та роз’яснення від ОВСП щодо необхідності пересилання та поширення новин лише з офіційних джерел, без скриншотів.

2.26 Заклик та роз’яснення від ОВСП не використовувати та не поширювати інформацію, пов’язану з астрологією, екстрасенсорикою, шаманством, магією тощо.

2.27 Заклик та роз’яснення від ОВСП щодо ролі «хороших ворогів» в соціальних мережах і ЗМІ.

2.28 Заклик громадян не вступати в соціальних мережах і на інших платформах у словесні перепалки з представниками країни-агресора.

2.29 Заклик громадян публічно не поширювати інформацію про геолокацію перебування.

2.30 Заклик громадян за можливості використовувати месенджерами на основі End-to-End Encryption чи Peer-to-Peer Connection.

2.31 Заклик громадян заблокувати функцію в соціальних мережах, яка дозволяє невідомими додавати в групи та чати.

2.32 Заклик громадян встановлювати на пристрої додатки лише з офіційних джерел.

2.33 Надання роз’яснень і порад громадянам про те, як безпечно поширювати інформацію про роботу волонтерів у кіберпросторі.

2.34 Надання роз’яснень і порад громадянам про те, як спілкуватися з близькими, які знаходяться в країні-агресорі, а також як їм донести правдиву інформацію.

2.35 Надання роз’яснень громадянам, як безпечно користуватися смартфоном під час окупації.

2.36 Надання роз’яснень, як ворог за допомогою кібервпливу навіює паніку, чому це небезпечно та як цьому протидіяти.

2.37 Надання роз’яснень, які сайти небезпечно використовувати в повсякденній діяльності та чому, які розширення файлів можуть стати загрозою для пристроїв і причини цього та яку небезпеку несе автоматичне підключення до WI-FI-точок у громадських місцях.

2.38 Надання роз’яснень щодо можливих ситуацій з мобільним зв’язком та як діяти під час них – як комунікувати з іншими за відсутності мобільного зв’язку та Інтернету: використовувати стаціонарний дротовий зв’язок або радіоприймач на батарейках; смартфон як пристрій радіозв’язку (рації) або створення mesh-мереж за допомогою відповідних додатків. Попередити, що такі способи спілкування не будуть конфіденційними.

2.39 Надання роз’яснень щодо прикладів автентичних посилань на інтернет-платформи.

2.40 Надання роз’яснень і інструкцій громадянам щодо користування VPN для власної безпеки.

2.41 Надання інструкцій громадянам, як заблокувати в месенджерах невідомих, потенційно небезпечних чи ворожих відправників, встановити першорядні параметри конфіденційності та захисту облікового запису за допомогою двофакторної автентифікації та автоблокування.

2.42 Надання інструкцій, як військовим користуватися інтернет-ресурсами.

2.43 Надання інструкцій, як отримати доступ до новин в разі відключення ворогом ефірного мовлення.

II. Міжнародні заходи

1. Нововведення

1.1 Впровадження онлайн-архіву для іноземної аудиторії з відображенням інформації про причини війни, останні відомості з офіційних джерел, ворожі злочини, способи допомоги.

1.2 Впровадження онлайн-журналу для іноземної аудиторії з представленням правдивих історій про героїчні вчинки та людські трагедії.

1.3 Впровадження на глобальних відеохостингах каналів з публікацією репортажів про новини мовами міжнародних партнерів.

1.4 Перевірка та розповсюдження переліку глобальних спеціалізованих ресурсів (Gofundme, JustGiving, Kickstarter, Indiego, MightyCause) для допомоги з боку міжнародних партнерів і громадян та протидії кібершахрайству.

1.5 Запит до всесвітніх організацій на ухвалення процесів і заходів, направлених на боротьбу на глобальному рівні з кібервпливом через порушення прав людини.

2. Співпраця

2.1 Співпраця з міжнародними союзами, альянсами, коаліціями, а також окремими країнами для запровадження санкцій (ліквідація супутникової, кабельної та Інтернет-трансляції) на їх територіях проти телеканалів, радіостанцій і видавництв, які поширюють дезінформацію противника.

2.2 Співпраця з міжнародними союзами, альянсами, коаліціями, а також окремими країнами для запровадження санкцій (заборона на в'їзд, замороження активів тощо) на їх територіях проти пропагандистів (ведучих, журналістів, політиків, блогерів тощо), які генерують і поширюють дезінформацію.

2.3 Співпраця з міжнародними союзами, альянсами, коаліціями, які координують і підтримують ЗМІ у поширенні достовірної інформації, щодо скасування членства представників країни-агресора.

2.4 Співпраця з представниками держав, у юрисдикції яких знаходяться супутники, що транслюють телеканали держави-агресора, з метою зупинки їх роботи.

2.5 Співпраця з глобальними компаніями ІТ-сектору для запобігання розповсюдження дезінформації противника на їхніх платформах.

2.6 Співпраця з керівництвом медіаресурсів і соціальних мереж щодо заблокування доступу до їхніх продуктів на території країни-агресора з метою недопущення поширення кібервпливу від пропагандистських джерел.

2.7 Співпраця з агентствами країн-партнерів для дослідження, виявлення та ліквідації «фабрик тролів» та ботоферм, які поширюють дезінформацію на користь ворожої країни; блокування облікових записів, які масово надсилають скарги та діяльність яких активізувалася під час кібервійни.

2.8 Співпраця з телеканалами та видавництвами іноземних партнерів для поширення новин на їх платформах мовою країни-жертви кібервпливу.

2.9 Співпраця з керівництвом соціальних мереж для пом’якшення вимог до контенту, який поширюють громадяни країни, з метою демонстрації правдивих наслідків військових дій. Запросити пришвидшений процес розблокування облікових записів, які начебто порушили правила розповсюдження дописів, пов’язаних з війною.

2.10 Співпраця з керівництвом соціальних мереж щодо впровадження для громадян функції закриття профілю від можливості перегляду незнайомцями.

2.11 Співпраця з керівництвом соціальних мереж щодо впровадження спеціального маркування (має однозначно повідомляти користувача, що це недостовірне джерело даних) облікових записів і дописів ворожих ЗМІ та пропагандистів, які на них працюють; утруднення їх пошуку з будь-якої точки світу шляхом зниження пріоритету облікових записів; попередження користувачів, що після переходу на ці сторінки їхній вміст не відповідає дійсності; заборони таким обліковим записам поширювати рекламу; блокування та видалення таких сторінок на запит уряду країни-жертви.

2.12 Співпраця з керівництвом соціальних мереж щодо відстеження та ліквідації штучно виготовлених і оброблених професійними інструментами медіаконтенту, які можуть представлятися як доказ певній інформації.

2.13 Співпраця з керівництвом соціальних мереж щодо заборони реєстрації облікових записів з країни, яка проводить кібервплив.

2.14 Співпраця з керівництвом соціальних мереж для впровадження на їхніх платформах функції перекладу новин з мови країни, яка є жертвою кібервпливу.

2.15 Співпраця з аерокосмічними компаніями для отримання супутникових знімків, які виступатимуть доказами в поширенні правдивої інформації.

2.16 Співпраця з провайдерами іноземних партнерів для трансляції на їх ресурсах національних телеканалів.

2.17 Співпраця з глобальними картографічними веб-сервісами для відключення функцій, які в реальному часі відображають відомості про завантаженість доріг та насиченість певного місця людьми.

2.18 Співпраця з рекламно-технологічними платформами з метою заборонити ворожим державним ЗМІ залучати рекламні оголошення через їх ресурси, а також публікувати контент, який заперечує, підтримує або виправдовує дії ворога.

2.19 Співпраця з провідними світовими ЗМІ про надання безкоштовного доступу до їх матеріалів про війну громадянам країни та її біженцям.

2.20 Співпраця з провідними світовими ЗМІ щодо відмови від цитування ворожих ЗМІ та пропагандистів, які на них працюють, під виглядом «альтернативної точки зору» та «дотримання свободи слова».

2.21 Співпраця з глобальними відеохостингами та стрімінговими сервісами щодо блокування на їх платформах джерел, що поширюють ворожу дезінформацію і пропаганду.

2.22 Співпраця з міжнародними компаніями, які надають інструменти для фактчекінгу.

ВИСНОВКИ

У результаті виконання всіх завдань дипломної роботи було досягнуто її мету – проведено дослідження небезпечного кібервпливу на суспільство (державу) під час гібридної війни та розроблено відповідний захист інформаційного сектору держави.

Для вирішення завдань було здійснено:

- розкрито необхідність захисту критичної інфраструктури в умовах кібервійни;
- простежено глобальні та локальні події, які стали передумовами кібервійни в українському віртуальному просторі;
- виконано аналіз заходів влади щодо забезпечення захисту інформаційного сектору;
- розроблено комплекс заходів захисту від кібервпливу на персонал критичної інфраструктури на основі такого, що відбувався протягом російського вторгнення на територію України з лютого по травень у 2022 році.

Втілений комплекс містить обов’язкові дії національного та міжнародного рівнів і, таким чином, втілює необхідний мінімум напрямків роботи компетентних органів влади та її очільників. Такі законні заходи будуть запобігати розповсюдженню всіх можливих проявів кібервпливу, серед яких поширення напівправди, спотворення фактів, раціоналізація ситуації, відкрита брехня, отруєння джерела, багатократне повторення, залякування, залучення красивих й успішних людей, гра на почуттях і переживаннях, контент із простими громадянами, махання прапорами, маніпуляція фактами, обвинувачення у фейках.

Розроблений комплекс обов’язково сприятиме поширенню серед персоналу критично важливих об’єктів інфраструктури, а також всього населення країни в цілому, коректних, істинних та справжніх відомостей про події в державі та поза нею. Отже, результат виконання дипломної роботи стане необхідною зброєю держави на кіберфронті для протидії ворожому кібервпливу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Resilience of Critical Infrastructure Protection in Europe (RECIPE) [Електронний ресурс] – Режим доступу: https://ec.europa.eu/echo/system/files/2017-11/recipe_guidelines.pdf.

3. Cyber security of critical infrastructures / L.A. Maglaras [та ін.]. – ICT Express, 2018 [Електронний ресурс] – Режим доступу: https://doi.org/10.1016/j.icte.2018.02.001.

4. Tariq N. Securing SCADA-based Critical Infrastructures: Challenges and Open Issues / Tariq N., Asim M., Khan F. A. – The 5th International Workshop on Cyber Security and Digital Investigation, 2019 [Електронний ресурс] – Режим доступу: https://doi.org/10.1016/j.procs.2019.08.086.

5. Future trend SCADA-related attack, mitigation and prevention tools / A. M. Arias [та ін.] – HyRiM, 2015 [Електронний ресурс] – Режим доступу: https://hyrim.net/wp-content/uploads/2017/12/HyRiM-D2.1-Future-Trend-SCADA%C3%94%C3%87%C3%89related-Attack-Mitigation-and-Prevention-Tools.pdf.

6. Zhu B. A Taxonomy of Cyber Attacks on SCADA Systems / Zhu B., Joseph A., Sastry S. – 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/document/6142258.

7. Cyber security management model for critical infrastructure / Limba T., Plėta T., Agafonov K., Damkus M. – Entrepreneurship and Sustainability Issues, 2017, [Електронний ресурс] – Режим доступу: https://doi.org/10.9770/jesi.2017.4.4(12).

8. The WIRED Guide to Cyberwar [Електронний ресурс] – Режим доступу: https://www.wired.com/story/cyberwar-guide.

9. Brangetto P. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations / Brangetto P., Veenendaal M. A. – 2016 8th International Conference on Cyber Conflict [Електронний ресурс] – Режим доступу: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

10. Hemsley K. E. History of Industrial Control System Cyber Incidents / Hemsley K. E., Dr. R. E. Fisher – INL, 2018 [Електронний ресурс] – Режим доступу: https://www.osti.gov/servlets/purl/1505628.

11. СБУ розслідує причетність російських спецслужб до кібератаки на органи державної влади України [Електронний ресурс] – Режим доступу: https://ssu.gov.ua/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy.

12. Казарян С. Кібератаки. Як Україна і світ борються з руйнівною діяльністю хакерів / Казарян С. – Telegraf.Design, 2022 [Електронний ресурс] – Режим доступу: https://telegraf.design/kiberataky-yak-ukrayina-i-svit-boryutsya-z-rujnivnoyu-diyalnistyu-hakeriv/.

13. Україна підозрює у кібератаці хакерів, пов'язаних із розвідкою Білорусі [Електронний ресурс] – Режим доступу: https://www.pravda.com.ua/news/2022/01/15/7320525/.

14. A Guide to Critical Infrastructure Security and Resilience – CISA, 2019 [Електронний ресурс] – Режим доступу: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

15. Указ Президента України від 13.02.2017 № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/32/2017#n2.

16. Вескус К. Технології в «Дію»: чим корисний досвід Естонії у впровадженні інновацій / Вескус К. – M!nd, 2020 [Електронний ресурс] – Режим доступу:

https://mind.ua/openmind/20211769-tehnologiyi-v-diyu-chim-korisnij-dosvid-estoniyi-u-vprovadzhenni-innovacij.

17. В один клік без черг та хабарів: Глава держави підписав указ щодо розвитку електронних послуг [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/news/v-odin-klik-bez-cherg-ta-habariv-glava-derzhavi-pidpisav-uka-56633.

18. Постанова Кабінету Міністрів України від 02.09.2019 № 829 «Деякі питання оптимізації системи центральних органів виконавчої влади» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/829-2019-%D0%BF#Text.

19. Постанова Кабінету Міністрів України 18.09.2019 № 856 «Питання Міністерства цифрової трансформації» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text.

20. Постанова Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

21. Дія – у дії! Презентовано мобільний застосунок Дія та Національну онлайн-платформу цифрової освіти [Електронний ресурс] – Режим доступу: https://thedigital.gov.ua/news/diya-u-dii-prezentovano-mobilniy-zastosunok-diya-ta-natsionalnu-onlayn-platformu-tsifrovoi-osviti.

22. Закон України від 16.11.2021 № 1882-IX «Про критичну інфраструктуру» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

23. Міністерство цифрової трансформації України [Електронний ресурс] – Режим доступу: https://www.kmu.gov.ua/catalog/ministerstvo-cifrovoyi-transformaciyi.

24. De Novo – еталонний провайдер хмарної інфраструктури VMware [Електронний ресурс] – Режим доступу: https://denovo.ua/.

25. GigaCloud: ідеальний хмарний сервіс для бізнесу [Електронний ресурс] – Режим доступу: https://gigacloud.ua/.

26. Тепер не лише De Novo. Стало відомо, куди «переїхала» Дія [Електронний ресурс] – Режим доступу: https://biz.nv.ua/ukr/tech/kudi-perejihala-diya-codi-data-centri-dlya-diji-viskub-novini-ukrajini-50194310.html.

27. Приклад №1 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/151103.

28. Приклад №2 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/groznyinform/9576.

29. Приклад №3 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/tass_agency/128384.

30. Приклад №4 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/medvedev_telegram/58.

31. Приклад №5 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/161268.

32. Приклад №6 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/80816.

33. Приклад №7 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/81019.

34. Приклад №8 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/82940.

35. Приклад №9 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/85695.

36. Приклад №10 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/86221.

37. Приклад №11 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/80063.

38. Приклад №12 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/SolovievLive/101191.

39. Приклад №13 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/79721.

40. Приклад №14 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/154124.

41. Приклад №15 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/156013.

42. Приклад №16 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/157767.

43. Приклад №17 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/159303.

44. Приклад №18 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/rian_ru/159634.

45. Приклад №19 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/tv360/80491.

46. Приклад №20 російського кібервпливу [Електронний ресурс] – Режим доступу: https://www.instagram.com/tv/CarHjqUAxmi/?utm_source=ig_web_copy_link.

47. Приклад №21 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/izvestia/88301.

48. Приклад №22 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/readovkanews/32321.

49. Приклад №24 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/riafan/94537.

50. Приклад №25 російського кібервпливу [Електронний ресурс] – Режим доступу: https://t.me/sputniklive/31750.

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИПЛОМУ

Тези наукових доповідей

1. Пархоменко І. Шматко В. Використання криптотехнологій при формуванні стегонаконтейнерів. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 12 червня 2020 року. Київ, 2020. С. 20-22.

2. Shmatko V., Bigdan A., Babenko T. AI-based network detection and response in Vectra networks implementation. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповодідей та тез; м. Київ, 15-16 квітня 2021 року. Київ, 2021. С. 10-11.

3. Shmatko V., Brailovskyi M. Forecasting cyberimpact on information sector of the state as a preventive method of protection against cyberwar. Прикладні системи та технології в інформаційному суспільстві: зб. тез доповідей і наук. повідомл. учасників V Міжнародної науково-практичної конференції (Київ, 30 вересня 2021 р.). Київ, 2021. С. 277-283.