Петляк Наталія Сергіївна, аспірант кафедри безпеки інформаційних технологій, Національний авіаційний університет; асистент кафедри кібербезпеки, Хмельницький національний університет.
Nataliia Petliak, PhD Student of IT-Security Academic Department, National Aviation University; Assistant of Department of Cyber Security, Khmelnytskyi National University.
E-mail: npetlyak@khmnu.edu.ua.
Orcid ID: 0000-0001-5971-4428.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, професор, професор кафедри Інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.
Yuliia Khokhlachova, candidate of technical sciences, professor, professor of the department of software engineering and cyber security of the State University of Trade and Economics.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

DOI: 10.18372/2410-7840.26.18842
УДК 004.056.5:327.88(470+571):477)

АНАЛІЗ СУЧАСНОГО СТАНУ КІБЕРАТАК В УКРАЇНІ ПІД ЧАС ВІЙНИ

Святослав Храмов, Іван Опірський

Актуальність проблеми кібербезпеки в Україні надзвичайно висока в контексті повномасштабного вторгнення. За останні роки кібератаки стали невід'ємною частиною гібридної війни, яка ведеться проти країни. Дослідження сучасного стану кібергресії в Україні є важливим завданням з погляду національної безпеки. Ця наукова робота має на меті ретельно проаналізувати структуру, тенденції та особливості кібератак, які спрямовані проти України під час військового конфлікту. Дослідження передбачає аналіз різноманітних форм і методів кібергресії, вивчення їхнього впливу на державу та ідентифікацію можливих заходів для захисту критичних інформаційних інфраструктурних об'єктів. Результати дослідження можуть послужити основою для розробки та впровадження ефективних стратегій з кібербезпеки, спрямованих на покращення захисту інформаційної безпеки країни в умовах військового конфлікту. Актуальність цієї роботи полягає в її потенційній здатності допомогти українському уряду та органам безпеки ефективно реагувати на виклики військового конфлікту в кіберпросторі. Для підтримки дослідження було проведено широкий аналіз літератури та статей, які надають інформацію про кібератаки під час війни. Крім того, були використані емпіричні дані про кіберінциденти, зафіксовані в Україні з початку конфлікту, що дозволило детально оцінити масштаби та специфіку загроз. Особливу увагу приділено аналізу типів кібератак, їх тактичних і стратегічних цілей, а також методів, які використовуються для їх реалізації. Дослідження також виявляє основні вразливості, які використовуються зловмисниками, і пропонує можливі шляхи їх усунення. Серед основних типів атак розглядаються DDoS-атаки, фішингові атаки, впровадження шкідливого програмного забезпечення, SQL-ін'єкції та інші. Крім того, розглядається вплив кібератак на різні сектори економіки та соціальної сфери, включаючи державне управління, енергетику, фінанси та інфраструктуру. Результати дослідження мають практичне значення для формування державної політики у сфері кібербезпеки. Вони можуть бути використані для розробки рекомендацій щодо підвищення захищеності інформаційних систем, удосконалення нормативно-правової бази та посилення міжнародного співробітництва в цій сфері. Дослідження також підкреслює необхідність підвищення кібергігієни серед населення та покращення підготовки спеціалістів з кібербезпеки.

***Ключові слова**: кібератаки, війна, типи кібератак, успішність кібератак, ІПСО, DDoS-атаки, прогнозування, методи протидії.*

ВСТУП

Постановка проблеми. У сучасному інформаційному суспільстві, де технологічний прогрес стає неодмінною складовою кожного аспекту життя, кіберпростір стає не лише ареною для технологічного розвитку, але й полем боротьби в контексті військового вторгнення рф на територію України. Одним із ключових аспектів цієї нової реальності є кібератаки під час війни, що визначаються використанням технічних засобів для завдання шкоди інформаційно-комунікаційним системам противника. Динамічний розвиток цього феномену викликає необхідність глибокого аналізу сучасного стану кібератак в умовах війни. Дослідження стану кібератак під час війни є актуальним, адже за показними кількість кібер-порушень безпекового стану в України стрімко зросли з початком повномасштабного вторгнення рф. Кібератаки почали використовуватись як елемент військової стратегії, стали загрозою глобальної безпеки, а необхідність кібератак стає критичною складовою військової діяльності та національної оборони. Метою дослідження є глибокий аналіз та систематизація су-

часного стану кібератак під час війни з метою розкриття їхніх технічних особливостей, виявлення стратегічних вимірів, залучення іноземного досвіду, виявлення успішності кібератак та визначення можливостей подолання наслідків. Завданням є висвітлення теоретичного змісту кібератак в Україні під час повномасштабного вторгнення; оцінка та успішність проведення кібератак у період війни; складання статистики. Дослідження ґрунтується на використанні діалектичного методу для вивчення сутності кібератак в України, а також на основі наукових розробок і публікацій формування та розвиток системи кібербезпеки. У статті використано методи наукового абстрагування, аналізу та синтезу, узагальнення, структурно-функціонального, емпірико-статистичного та порівняльного аналізу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дана наукова робота зосереджена на аналізуванні ранніх наукових робіт, їх систематизація й виявлення викликів для наступних досліджень. Публікації досліджують різноманітність кіберагресій та їхній вплив на українську інфраструктуру. Особлива увага приділяється таким методам, як DDoS-атаки, фішинг, розповсюдження вірусів та іншим видам шкідливих програм. Дослідження виявляють тенденції зростання частоти та складності кібератак, а також зміни у використанні технологій та тактик сучасних хакерських груп, а також пропонуються різні стратегії та заходи з підвищення кібербезпеки, включаючи розвиток захисних технологій, підвищення кваліфікації фахівців та міжнародне співробітництво.

Актуалізована проблема забезпечення кібербезпеки України в умовах зростання викликів та загроз в інформаційному просторі розглянута у статті С. Оніщенко, А. Глушко [3]; Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак розглінута у роботі Р. Грищук, В. Охрімчук [3]; Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні О. Бодунов [10]; Забезпечення захисту кіберпростору в провідних країнах світу С. Паламарчук [4].

ПОСТАНОВКА ЗАВДАННЯ

Основними завданнями представленої наукової роботи є проведення аналізу літературних джерел та наукових публікацій, що стосуються кібербезпеки та кібератак в Україні під час війни. Зібрати та систематизувати статистичні дані про кібератаки, що відбулися в Україні з початку військового конфлікту; визначити основні цілі та об'єкти кібератак, що спрямовані на Україну; проаналізувати типи та методи кіберагресій, використовувані сторонами конфлікту; вивчити наслідки кібератак для національної безпеки, економіки та соціальної сфери України; розглянути заходи протидії та захисту від кіберагресій, які застосовуються українськими владними та недержавними структурами; сформулювати висновки щодо поточного стану кібербезпеки в Україні та розробити рекомендації щодо подальших заходів для підвищення захищеності інформаційної інфраструктури країни в умовах війни.

ОСНОВНА ЧАСТИНА

Статистика кібератак під час війни

Сьогодні використання інтернет-технологій стало необхідною частиною повсякденного життя для більшості людей. Державні і приватні структури активно впроваджують електронний документообіг, банківські установи використовують автоматизовані електронні системи, а залізничний транспорт теж залежить від електронних засобів зв'язку. Використання інтернет-комунікацій значно полегшує щоденне життя громадян і сприяє покращенню роботи органів влади, місцевого самоврядування, підприємств і організацій.

У сучасних умовах важко переоцінити вплив інформаційної війни, яка приносить не менше збитків, ніж війна на полі бою. Україна, реагуючи на цю загрозу, вже розпочала процес удосконалення чинного кримінального та кримінально-процесуального законодавства, спрямований на притягнення до відповідальності осіб, зайнятих кіберзлочинами.

Після повномасштабного вторгнення росії на територію України кількість правопорушень у сфері інформаційних технологій значно зросла (рис. 1). Країна-агресор активно використовує інтернет-технології для дезінформації, поширення пропаганди та впровадження ворожих ідей, зокрема щодо вторгнення в Україну. У зв'язку з цим, уряд України приймає заходи щодо адаптації законодавства, щоб боротися із цим викликом та ефективно притягати до відповідальності тих, хто порушує кібербезпеку [1].

В період від січня 2022 року до вересня 2023 року було документовано майже 4 тисячі кібератак на територію України. Це втричі перевищує обсяг атак, зафіксований до початку збройного конфлікту. рф координує та виконує деструктивні кібератаки, спрямовані на Україну, включаючи вторгнення в її інформаційні систе-

ми, інфільтрацію в мережу та здійснення шпигунської діяльності в країнах, розглядуваних як союзники української держави. Додатково, російська сторона впроваджує операції кібервпливу, спрямовані на систематичний вплив на свідомість та переконання громадян у різних країнах світу. російська федерація використовує кібератаки як інструмент впливу, зосереджуючись не лише на Україні, а й на Сполучених Штатах та Польщі, оскільки вони виступають як координатори значної частини матеріально-технічного забезпечення військової та гуманітарної допомоги для України. Практика також свідчить, що злочинна діяльність російських хакерів націлена на країни Балтії та в останній час розширюється на Данію, Норвегію, Фінляндію, Швецію, Туреччину та інші країни НАТО, включаючи атаки на комп'ютерні мережі міністерств закордонних справ. У другій половині 2022 року російські хакери активно націлювалися на логістичні та транспортні компанії, як в межах, так і за межами України. Цільовими об'єктами атак є не лише уряди, але й аналітичні центри, гуманітарні організації, IT-компанії, постачальники енергії та інші важливі об'єкти інфраструктури. За даними експертів, лише 29% кібератак росіян виявилися успішними протягом активної фази війни [3].

Рис. 1. Динаміка збільшення кібератак в Україні за період 2019-2022 років

Україна активно взаємодіє з міжнародною спільнотою у сфері кібербезпеки. Під час візиту до штаб-квартири НАТО українська делегація поділилася досвідом кібервійни та висловила інтерес до майбутньої співпраці з НАТО в цій області, представивши свої потреби та пропозиції.

Під час візиту до Брюсселя обговорювались організація третього раунду кібердіалогу між Україною та ЄС, успіхи в гармонізації кібербезпеки України із стандартами ЄС, а також перспективи подальшої співпраці. Україна активно брала участь у щорічних навчаннях НАТО з взаємосумісності та розпочала співпрацю з численними аналітичними структурами Європи.

Аналіз типів та об'єктів впливу атак на Україну

Протягом 2023 року українські експерти з безпеки зафіксували та аналізували 1105 кіберінцидентів, що є на 62,5% більше, ніж у попередньому році. Система, яка використовується для відслідковування та аналізу кіберзагроз, виявила 133 мільйони подій, які викликали підозри, та 148 000 критичних інцидентів. Загалом було оброблено близько 18 мільярдів подій. Протягом останнього року до системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було включено 24 нових об'єкти, представлених різними секторами, зокрема урядовим (22), енергетичним (1) та військовим (1). Серед автономних систем, які найчастіше брали участь у атаках, можна відзначити Google, Hurricane, Google Cloud Platform, Cloudflarenet та DigitalOcean-ASN [2].

На кінець 2023 року великий мобільний оператор України "Київстар" став свідком серйозного перебою у роботі через хакерську атаку. Протягом понад доби фахівці працювали над відновленням мережі, і повністю відновити 100% послуг вдалося за тривалий тиждень. Кібератака на "Київстар" призвела до руйнування приблизно 40% інфраструктури компанії, особливо постраждавши прошарок мережі.

Тільки за період перших чотирьох місяців війни було виявлено 796 кібератак, основними секторами яких є: уряд і місцеві органи (179 атак), сектор безпеки й оборони (104 атаки), фінансовий сектор (55 атак), комерційні організації (54 атаки), енергетичний сектор (54 атаки), а також інші – 350 атак [5]. Також під час цього процесу кіберзлочинці активно залишають у своєму полі зору транспортну інфраструктуру та галузь телекомунікацій.

Кіберхакери використовують різноманітні методи для здійснення атак на інформаційні системи та мережі. До основних методів можна віднести фішинг (відправка шахрайських повідомлень з метою отримання конфіденційної інформації), малвару (впровадження шкідливого програмного забезпечення для збору даних або завдання шкоди), деніал-оф-сервіс атаки (намагання перевантажити ресурси мережі), SQL-ін'єкції (внесення змін у базу даних для отримання несанкціонованого доступу), атаки на ідентифікатори та паролі, та інші техніки, спрямовані на злам інформаційної безпеки та завдання збитків.

Наведені найпоширеніші методи втручання в кібербезпеку України за час повномасштабного вторгнення рф (рис. 2). За даними Державної служби спеціального зв'язку та захисту інформа-

ції за період перших чотирьох місяців війни на Україну було направлено 242 кібератаки методом збору інформації, що є 30,4% до основної кількості кібератак за перші чотири місяці повномасштабного вторгнення; 192 – методом шкідливого програмного код (24,1%); 92 (11,6%) – втручання; 82 (10,3%) – спроби втручання; 56 (7,0%) – порушення доступності; інші – 47%.

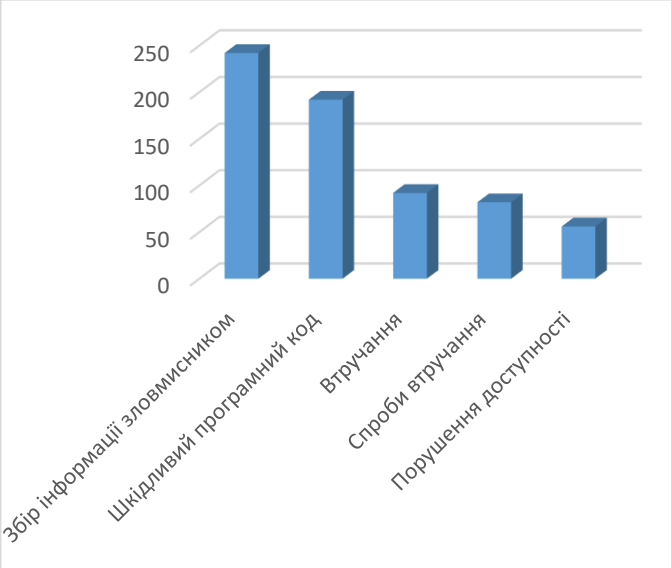

Рис. 2. Найпоширеніші методи кібератак в Україні

Успішність реалізації атак в залежності від типу

2022 рік визначається як період першої світової кібервійни, особливістю якого є значна кількість хакерських атак на Україну та її міжнародних союзників.

В ході сучасної конфлікту стає очевидним, що хакерські групи тісно взаємодіють з апаратом безпеки країни-агресора. Діяльність цифрових найманих чітко координується з військовими операціями російської армії на полі бою, а також впровадженням інформаційно-психологічних операцій або ІПСО. Все це становить важливий елемент стратегії росії в гібридній війні. Кількість кібератак щоденно зростає, а їх структура стає більш складною. За даними Державної служби спеціального зв'язку та захисту інформації, лише протягом грудня 2022 року вони відбили майже 400 потужних DDoS-атак і зафіксували понад 170 тисяч спроб експлуатації вразливостей, тисячі заражень та сотні сканувань. Це підтверджує факт, що Україна в 2022 році посідає друге місце у світі за кількістю кібератак, тільки поступаючись США [6].

Особливо виділяється підвищення активності вірусів-вимагачів, або Ransomware, у 2022 році. Цей вид шкідливого програмного забезпечення призначений для блокування доступу до файлів або IT-систем організацій. Зазвичай зловмисники вимагають викуп у обмін на ключ для розшифрування даних.

Найбільш поширеними серед кіберзлочинців були використані шкідливі програми, такі як SmokeLoader, Agent Tesla, Snake Keylogger, Remcos і Formbook.

Упродовж серпня-вересня 2023 року угруповання хакерів неодноразово намагалося викрасти десятки мільйонів гривень. З 2 по 6 жовтня 2023 року в Україні зафіксовано принаймні чотири хвилі кібератак. Зафіксовано, що атаки проводилося за допомогою шкідливої програми SmokeLoader, і це було виконано угрупуванням UAC-0006. Характерний стратегічний план зловмисної групи UAC-0006 включає в себе зараження комп'ютерів, які використовуються для обліку, з метою втручання у фінансову діяльність, а також вивчення та викрадення автентифікаційних даних для незаконних транзакцій [7].

За період липня-вересня 2023 року 97 інцендентів кібератак на українську систему безпеки. На D-Dos- атаки припадає 89% усіх інцендентів, найбільші цільові сектори – державне управління, ЗМІ, ІКТ, фінанси і торгівля. BlueNet Russia і Phoenix виходять на друге і третє місце серед найактивніших загроз. В порівнянні, в рф , за період ливня-вересня 2023 року, сталося всього 13% інцендентів, а в 37 інших країнах за статистикою – 472 (табл. 1).

Таблиця 1

Кількість успішності кібератак за період липня-вересня 2023р, в Україні, рф та інших країнах світу

Країна	Дата атаки					
	01.07.	29.07.	05.08.	26.08.	02.09.	30.09.
Україна	11	5	6	8	8	1
російська федерація	1	0	1	1	3	0
Інші країни	15	31	30	33	67	34

Головною метою нанесення кібератак є надання збитків країні, підприємству, тощо. За даними дослідження IBM Global Average Data Breach, у 2022 році глобальні втрати даних від кібератак становили 4,4 мільйона доларів, порівняно з 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році. За 2020-2021 роки середні річні витрати на витік даних зросли, ймовірно, через пандемію COVID-19. У 2022 році вони склали 4,35 мільйона доларів, що на 2,6% більше, ніж у 2021 році (4,24 мільйона доларів). Вартість витоку в галузі охорони здоров'я зросла на 42% з 2020 року. Охорона здоров'я продовжує бути лідером за витратами на витік даних вже 12 років

поспіль. На початку 2023 року зафіксовано зменшення прибутковості для хакерських атак у порівнянні з попереднім роком 2022. Це явище пояснюється адаптацією світової спільноти до програм-вимагачів та звичайних схем атак, що призвело до зменшення кількості компаній, які оплачували викуп за даними. Замість цього, потерпілі стали усвідомлювати важливість вивчення заходів безпеки та інвестування в захист своїх інформаційних систем. Аналіз даних свідчить про зміну динаміки в цьому напрямку, що вказує на імовірність статистичної помилки в попередніх висновках. У минулому році кількість виплат викупів значно збільшилася, майже подвоївшись, до рівня 1,1 мільярда доларів, у порівнянні з 567 мільйонами доларів у 2022 році. Дана статистика наведена на графіку (рис. 3), усі наведені показники відображені у млн. дол. США.

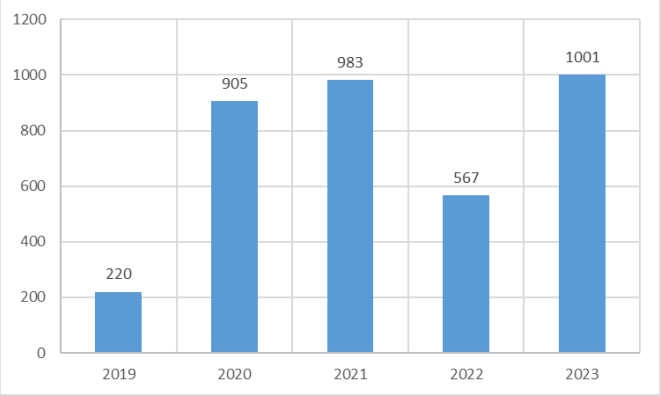

Рис. 3. Тенденції отриманих доходів від кібератак, за період 2019-2023 років

Корпорація Recorded Future, яка спеціалізується на моніторингу та аналізі кіберзагроз, оприлюднила звіт про з'яву 538 нових варіацій програм-вимагачів протягом 2023 року. Видатні кіберзлочинні групи тепер зосереджують свою увагу на великих організаціях з високою стійкістю для вимагання більших сум викупу. Крім того, спостерігається значний зріст використання програм-вимагачів як послуг (RaaS), що дозволяє навіть користувачам з обмеженим технічним досвідом наймати вірусні програми в оренду за певну вартість, яку вони сплачують розробникам шифрувального програмного забезпечення. Є підстави вважати, що обсяг та наслідки витоків даних продовжать зростати в майбутньому. Протягом останніх років спостерігається збільшення вартості витоку інформації, що з 2020 року зросло на 15,3%. Також спостерігається зростання числа значних кібератак: у 2020 році їх було 1120, а вже у 2023 році – 1659. Зрозуміло, що збільшення кількості витоків має вплив на розмір завданих збитків. За політичної та геополітичної нестабільності в Україні, активної військової агресії зі сторони в рф, складно робити висновки щодо прогнозування кібератак станом на 2024 рік.

Приблизне значення даного показника було статистично обраховано методом експоненційного зглажування, в якому бралися дані за попередні 4 роки і зменшувалась ступінь врахування. Таким чином, ми отримали показники, продемонстровані (табл. 2), а також їх тенденція на графіку (рис. 4).

Таблиця 2

Статисичне передбачення кіберзагроз на територію України на 2024 рік

Рік	Показник	Передбачення	Найнижчий показник	Найвищий показник
2020	1120	-	-	-
2021	1300	-	-	-
2022	1500	-	-	-
2023	1659	1659	1659,00	1659,00
2024	-	1844,481081	1826,50	1862,47

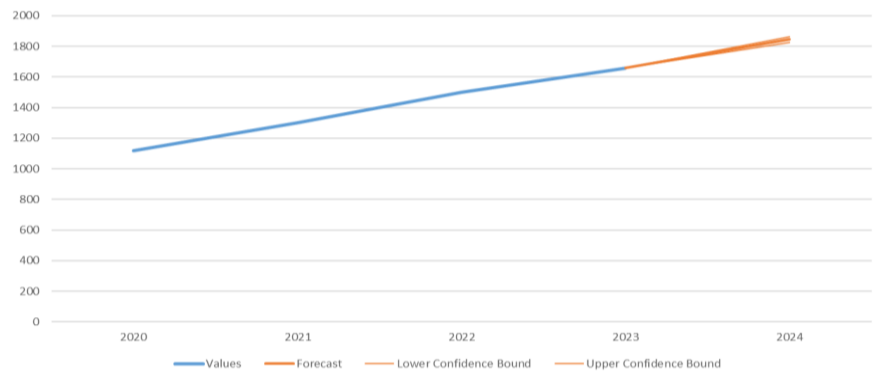

Рис. 4. Динаміка прогнозованих кіберзагроз в Україні, станом на 2024 рік

Отже, обрахунок показав, що число можливих кібератак в Україні на 2024 рік, становить 1844,5 атак, що є на 12% більшим, ніж попереднього року. Динаміка зображена на рисунку 4.

Прогноз на 2024 рік показує додаткове зростання кількості атак, що може вказувати на подальше загострення ситуації у сфері кібербезпеки. Це може бути спричинене різноманітними факторами, включаючи технічний розвиток зловмисників, нові методи атак та недоліки у захисті інформації. Сектору ІТ-технологій України слід підкреслити необхідність підвищення уваги до кібербезпеки в Україні та вжиття відповідних заходів для захисту інформації та критичних інфраструктурних об'єктів.

Дослідження проблематики успішності атак здійснених в Україні під час війни

Кіберзагрози для України поділяються на два основних рівні. Перший – це "класичні" кіберзлочини, що включають як новаторські, так і вже відомі атаки, для реалізації яких використовуються сучасні інформаційні технології. Другий рівень охоплює злочини, які виражають геополітичну боротьбу або мають потенціал вплинути на політичне становище держави, такі як хактивізм, кібершпигунство та кібердиверсії. Обидва рівні можуть використовувати схожі техніки атак, наприклад, фішингові методи для виведення грошей громадян або для проведення кібершпигунства.

Прикладом хактивізму в Україні стали події, пов'язані із закриттям файлообмінного сервісу ex.ua, які викликали DDoS-атаки на державні вебресурси. Ці події висвітлили непідготовленість країни до кіберагресії та підкреслили потребу у зміцненні захисту в інформаційній сфері [8].

23 лютого 2022 року, за день до початку російського вторгнення в Україну, стали свідками нових атак на веб-ресурси державного та банківського сектору. Приблизно о 16:00 почались пошкодження веб-сайтів Верховної Ради, Кабінету Міністрів України, Міністерства закордонних справ, Служби безпеки України та інших. Міністерство освіти і науки, з метою запобігання кібератакам, призупинило доступ до свого веб-сайту.

Атака сталася через інфікування сотень комп'ютерів вірусом HermeticWiper, який був створений ще 28 грудня 2021 року. 24 лютого вночі та вранці, під час наступу російських військ, було проведено атаки на веб-сайт Київської обласної державної адміністрації, а деякі інші ресурси були відключені для збереження даних. На платформах i.ua та meta.ua, за інформацією Державної служби спеціального зв'язку та захисту інформації, розсилаються численні електронні листи із фішинговими посиланнями на особисті адреси українських військових та їхніх родичів. Дослідження компанії Google вказує на те, що фішингова кампанія виходила з території Білорусі. Паралельно з українськими посадовцями, фішингові листи отримували також польські військові, з моменту появи українських біженців на польському кордоні.

Таблиця 3

Основні методи здійснення кібератак: Вразливість-Загроза-Вплив-Метод

Вразливість	Загроза	Вплив	Метод здійснення
Відсутність належного захисту DDoS-атак	Перевантаження сервісів	Відмова в обслуговуванні, зупинка сервісів	DDoS-атаки за допомогою ботнетів
Незахищеність внутрішньої мережі	Поширення шкідливого ПЗ	Параліч систем, втрата даних	Розповсюдження вірусів та троянів
Використання старих версій ПЗ	Експлуатація вразливостей ПЗ	Компрометація системи, крадіжка даних	Експлуатація відомих вразливостей (наприклад, CVE)
Недостатній контроль доступу	Неавторизований доступ	Компрометація конфіденційних даних	Використання вкрадених або вгаданих паролів
Недостатня надійність шифрування даних	Перехоплення комунікацій	Компрометація конфіденційних даних	Атаки типу "людина посередині" (MITM)
Неналежний моніторинг і реагування	Тривале несанкціоноване проникнення	Значні втрати даних, фінансові втрати	Тривале проникнення (APT-атаки)

У відповідь на попередні кібератаки, Михайло Федоров оголосив про створення ІТ-армії, яка включатиме експертів різних сфер для протидії дезінформації в Інтернеті та для здійснення кібератак на російські веб-сайти. Через кілька годин були запроваджені атаки на десятки російських банків, державних, інформаційних ресурсів та інших веб-сайтів. Деякі російські медіа почали транслювати українські пісні.

12 грудня 2023 року відбувся значущий збій у роботі найбільшого мобільного оператора Укра-

їни "Київстар". Внаслідок цього абоненти по всій країні втратили доступ до мобільного зв'язку та Інтернету, при цьому неможливо було перейти до мереж інших операторів у рамках внутрішньоукраїнського роумінгу. Крім того, сайт та застосунок "Київстар" також перестали працювати. В результаті цього зв'язок був втрачений для 24 мільйонів абонентів. Збої стали причиною серйозних інфраструктурних проблем по всій території України.

Подібних атак в період з початку повномасштабного вторгнення і по сьогодення було дуже багато, але майже всі вони мають спільні методи, які робили їх успішними. Такі методи продемонстровані (табл. 3).

За чотири роки роботи CDTO активно займається сферою кібербезпеки, реалізуючи понад 20 проектів в різних регіонах.

Наприклад, у 2023 році в Полтавській області були проведені перші регіональні командно-штабні навчання (ТТХ), у Волинській області – перші кіберзмагання у форматі CTF, а на Черкащині була впроваджена система "Безпечна школа".

У зв'язку з непередбачуваними загрозами кібербезпеки, особливо в умовах війни, важливо розуміти, що ефективний захист вимагає взаємодії трьох основних елементів: людей, процесів та технологій. Наш досвід свідчить, що освіта та розвиток навичок кібергігієни є вирішальними в аспекті протидії загрозам у цій області [9].

Можливі заходи і методи підвищення ефективності протидії кібератакам в Україні

На сьогоднішній день Україна немає гарантій щодо відсутності нових кібератак, тому як державним, так і комерційним структурам важливо приділити увагу запобіганню подібних нападів і успішному протистоянню їм у майбутньому. Ефективним способом це зробити є встановлення єдиної системи обміну інформацією в українському кіберпросторі. Подібні системи вже успішно функціонують у багатьох країнах Європи. Наприклад, в Естонії, яка в першу чергу постраждала від російських кібератак у 2007 році, така система діє з 2011 року. Міжнародний досвід демонструє, що ефективний обмін інформацією є ключовим у протистоянні кібератакам. Це дозволяє оперативно реагувати на виявлені загрози, обмінюватися досвідом та спільно боротися з ними. Фахівці відстежують підозрілі або несподівані події у кіберпросторі, аналізують їх і прогнозують можливі кібератаки, щоб вчасно попередити їх.

Для відповіді на мінливі вимоги у сфері кібербезпеки Україні необхідно розглядати два шляхи. Перший шлях полягає у вдосконаленні системи вищої освіти. Спеціалізована спеціальність "Кібербезпека" в галузі інформаційних технологій не забезпечує всього спектру знань і навичок, які потрібні на ринку праці. Розширення освітніх можливостей потребує співпраці з Міністерством освіти, але цей процес може бути тривалим. Другий шлях полягає у впровадженні міжнародних стандартів та кращих світових практик у сфері кібербезпеки. Розширення переліку професій для кіберспеціалістів та створення системи оцінювання фаху є ключовими напрямками [10]. Це дозволить розширити ринок праці для фахівців і забезпечить роботодавцям необхідними кадрами. Держспецзв'язку активно працює над цими ініціативами, включаючи створення кваліфікаційних центрів для професійних іспитів та надання освітніх послуг.

Запобігання наслідкам таких інцидентів стає щорічно все складнішим завдяки зростаючій складності та координації кіберзлочинності. Це робить виявлення та захист від неї надзвичайно важкими завданнями для організацій. Проте, на допомогу може прийти належно організована структура IT-інфраструктури та використання перевірених рішень у сфері кібербезпеки.

Україна активно співпрацює зі своїми партнерами у галузі кіберзахисту, і це має важливе значення не лише для самої країни, а й для міжнародного співтовариства. Досвід України у протидії кібератакам російського агресора допомагає іншим країнам у побудові ефективних систем захисту. Міжнародні заходи з кібербезпеки, такі як конференції FIRST та Black Hat-2022, свідчать про значний інтерес спільноти до досвіду України. Україна також активно обмінюється інформацією про кіберзагрози з партнерами, що підтверджується угодами про взаєморозуміння, укладеними з Республікою Словенія, Сполученими Штатами Америки та Республікою Польща.

Алгоритмом протидій кіберзагроз в Україні може стати даний план, розроблений авторами наукової представленої наукової публікації:

1. Ідентифікація та аналіз загрози.

1.1 Виявлення загрози: зібрати дані про виявлену загрозу, використовуючи системи моніторингу, IDS/IPS, антивірусні програми та інші засоби.

1.2 Аналіз загрози: провести детальний аналіз загрози для визначення її природи, методу проникнення та потенційних наслідків.

2. Ізоляція загрози.

2.1 Ізоляція уражених систем: відключити уражені системи від мережі для запобігання подальшому поширенню загрози.

2.2 Контроль доступу: обмежити доступ до уражених систем для запобігання несанкціонованому втручанню.

3. Ліквідація загрози.

3.1 Видалення шкідливого програмного забезпечення: використовувати антивірусні програми та інші засоби для видалення шкідливого програмного забезпечення та очищення систем.

3.2 Виправлення вразливостей: впровадити необхідні патчі та оновлення для закриття вразливостей, що дозволили реалізувати атаку.

4. Відновлення систем.

4.1 Відновлення даних: відновити дані з резервних копій, якщо вони були пошкоджені або втрачені внаслідок атаки.

4.2 Перевірка цілісності систем: перевірити цілісність систем та даних після ліквідації загрози та відновлення.

5. Оцінка та покращення захисту.

5.1 Аналіз інциденту: провести детальний аналіз інциденту для виявлення причин, наслідків та вразливих місць у системі захисту.

5.2 Покращення захисту: впровадити додаткові заходи безпеки, оновити політики та процедури, провести навчання персоналу на основі отриманих висновків для запобігання подібним інцидентам у майбутньому.

На основі цього алгоритму слід побудувати блок-схему, яка покаже які етапи алгоритму забезпечать протидію загрозам. Нижче зображена така блок-схема (рис. 5).

Ця блок-схема представляє процес ефективного управління загрозами в інформаційній системі, від виявлення та аналізу до повної нейтралізації загрози. Вона акцентує увагу на важливості послідовних дій для забезпечення безпеки та цілісності системи. Процес завершується аналізом інциденту і впровадженням заходів для покращення захисту та запобіганні виникненню загроз у майбутньому.

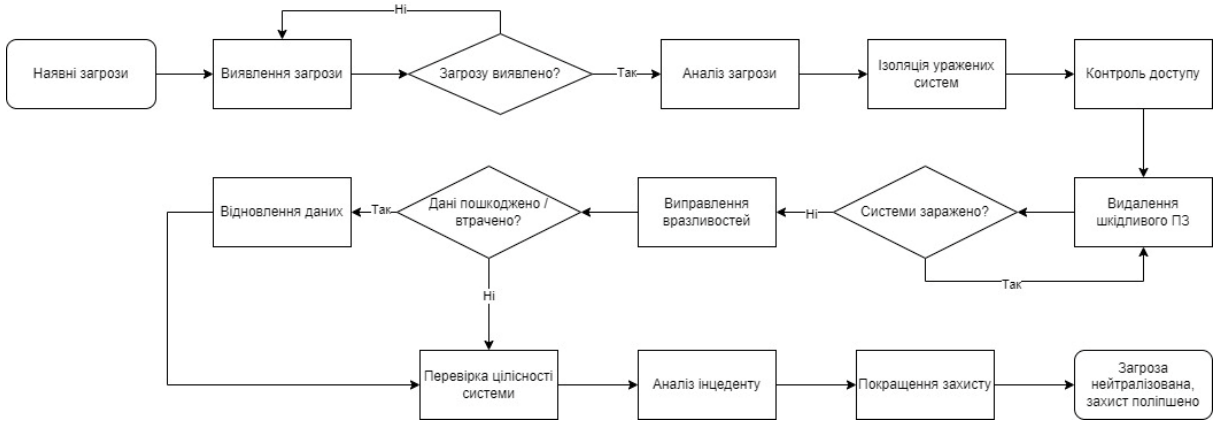

Рис. 5. Алгоритм протидії успішним атакам

ВИСНОВКИ

У висновку можна підкреслити, що сучасний стан кібератак в Україні під час війни свідчить про серйозні загрози для національної кібербезпеки. Аналіз інцидентів показує, що Україна постійно стикається зі складними кіберзагрозами, зокрема від російської федерації. Повномасштабне вторгнення рф створило сприятливі умови для зростання кібератак та інших кіберзлочинних дій. Підвищення активності кіберзлочинців свідчить про необхідність посилення заходів кібербезпеки та впровадження нових технологій захисту.

Загальний аналіз показує, що рівень кіберзагроз у Україні є високим, а їхні наслідки можуть бути катастрофічними для держави та її громадян. В умовах війни кібератаки стають ефективним засобом ведення гібридної війни, спрямованої на дестабілізацію країни та підірвання національної безпеки. Протидія кіберзагрозам вимагає комплексного підходу та систематичних заходів з боку держави, бізнесу та громадськості.

Для забезпечення ефективного захисту важливо розвивати національну кіберінфраструктуру, вдосконалювати законодавство у сфері кібербезпеки та зміцнювати співпрацю з міжнародними партнерами. Також необхідно вдосконалювати системи моніторингу та виявлення кіберзагроз, навчати персонал у сфері кібербезпеки та постійно оновлювати заходи захисту.

У цьому контексті важливо також підвищувати інформаційну грамотність громадян та популяризувати питання кібербезпеки серед широко-

го загалу. Тільки за умови спільних зусиль та постійного розвитку кіберінфраструктури Україна зможе успішно протистояти сучасним кіберзагрозам під час війни та забезпечити національну безпеку.

ЛІТЕРАТУРА

[1]. Гавловський, В. Д. (2019). Захист інформації шляхом посилення ефективності протидії кібератакам. Інформація і право, (3), 105-110.

[2]. Леонов Б.Д., Серьогін В.С. (2019). Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. Інформація і право. № 4(31). С. 98-106.

[3]. Онищенко, С. В., & Глушко, А. Д. (2020). Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації.

[4]. Паламарчук, С. А., Шемендюк, О. В., Ляшенко, Г. Т., & Ткач, В. О. (2020). Забезпечення захисту кіберпростору в провідних країнах світу. Збірник наукових праць Військового інституту телекомунікацій та інформатизації, С. 58-64.

[5]. Пеньков В.І., Штонда Р.М., Гук О.М., Мальцева І.Р., Черниш Ю.О. (2017) Методи та засоби протидії шкідливому програмному забезпеченню. Сучасні інформаційні технології у сфері безпеки та оборони. № 2 (29). С. 58-64.

[6]. Поляков, О. М. (2023). Сучасні тренди виявлення та протидії застосуванню шпигунських та шкідливих програм. Інформація і право, (2 (45)), С. 125-138.

[7]. Україна – одна з головних цілей для кібератак у світі. Як захиститися? Розповідаємо з прикладами – Delo.ua. (2023). Останні новини України та світу онлайн, Головний діловий портал Delo.ua. https://delo.ua/telecom/ukrayina-odna-z-golovnix-cilei-dlya-kiberatak-u-sviti-yak-zaxistitisya-rozpovidajemo-z-prikladami-412454/.

[8]. Як забезпечити захист кіберпростору України на тлі збройної агресії рф. (2023). АрміяInform, Інформаційне агентство АрміяInform. https://army-inform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/.

[9]. Як захистити Україну від кібератак. (2017). LB.ua. https://lb.ua/blog/mykola_kozlov/375661_yak_zahistiti_ukrainu_vid_kiberatak.html.

[10]. Ms.detector.media. (2022). Liga.net: За три роки кількість кібератак на Україну зросла в 5 разів. Більшість з них – російські. https://ms.detector.media/kiberbezpeka/post/28989/2022-02-19-liga-net-za-try-roky-kilkist-kiberatak-na-ukrainu-zrosla-v-5-raziv-bilshist-z-nykh-rosiyski/.

[11]. Onyshchenko, S., & Hlushko, A. (2022). Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Науковий журнал «Економіка і регіон», (1 (84)), С. 13-20.

ANALYSIS OF THE CURRENT STATE OF CYBERATTACKS IN UKRAINE DURING THE WAR

The urgency of the cybersecurity problem in Ukraine is extremely high in the context of a full-scale invasion. In recent years, cyberattacks have become an integral part of the hybrid war waged against the country. The study of the current state of cyber aggression in Ukraine is an important task from the point of view of national security. This scientific work aims to carefully analyze the structure, trends, and features of cyberattacks against Ukraine during the military conflict. The study involves the analysis of various forms and methods of cyber aggression, studying their impact on the state, and identifying possible measures to protect critical information infrastructure facilities. The study's results can form the basis for the development and implementation of effective cybersecurity strategies aimed at improving the protection of the country's information security in conditions of war. The relevance of this work lies in its potential to help the Ukrainian government and security agencies effectively respond to the challenges of military conflict in cyberspace. To support the study, a broad analysis of the literature and articles providing information on cyber-attacks during the war was conducted. Additionally, empirical data on cyber incidents recorded in Ukraine since the beginning of the conflict were used to comprehensively assess the scope and specifics of the threats. Special attention is paid to the analysis of types of cyberattacks, their tactical and strategic objectives, and the methods used for their implementation. The study also identifies key vulnerabilities exploited by attackers and suggests possible ways to mitigate them. The main types of attacks considered include DDoS attacks, phishing attacks, malware deployment, SQL injections, and others. Moreover, the impact of cyberattacks on various sectors of the economy and social sphere, including government administration, energy, finance, and infrastructure, is examined. The results of the study are practically significant for shaping national cybersecurity policy. They can be used to develop recommendations for enhancing the security of information systems, improving the regulatory framework, and strengthening international cooperation in this field. The study also emphasizes the need to increase cyber hygiene among the population and improve the training of cybersecurity specialists.

Keywords: cyberattacks, war, types of cyberattacks, success of cyberattacks, PSYOP, DDoS-attacks, forecasting, methods of counteraction.

Храмов Святослав Олександрович, студент інституту комп'ютерних технологій, автоматики та метрології, кафедри захисту інформації Національного університету «Львівська політехніка».

Khramov Sviatoslav, student of the Institute of Computer Technologies, Automation and Metrology, Department of Information Security, National University "Lviv Polytechnic".

E-mail: sviatoslav.khramov.kb.2022@lpnu.ua.
Orcid ID: 0009-0004-6486-8631.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.26.18843
УДК 004.415.05

МЕРЕЖЕВОЦЕТРИЧНІ ВІЙНИ – ВІЙНИ СУЧАСНОСТІ

Володимир Артемов, Володимир Хорошко

В статті розглядається теорія мережевоцентричної війни та її вплив на сучасність. Вона була розроблена у другій половині XX сторіччі та широко використовується у війнах XXI сторіччя. Сутність концепції мережевоцентричної війни можливо переоформлювати наступним чином це війна «сліпого» проти «зрячого». Фізична сила «сліпого» - бойова міцність класичних збройних сил, які не користуються перевагами мережево-центричних підходів, що не гарантує переваги в сучасному бою. Це завідомо програшна ситуація. Мережевоцентричної війна складається з 3-х решіток–підсистем: інформаційної, сенсорної (тобто розвідувальної) і бойової. Але її основу складає інформаційна підсистема, цілями якої, виходячи з концепції є так звані кільця Уордена. Використовуючи теорію мережевоцентричної війни та застосовуючи тактику гібридної війни, РФ захопила Крим та окупувала Донбас. А 24 лютого 2024 року росія розпочала війну проти України, причому повторюючи свої дії при агресії проти Грузії у 2008 році. Тобто, починаючі з кібератак на державні установи та центри керування державою. Але рф використовуючи елементи мережевоцентричної війни, воює як воювали у Другій світовій війні. Україна застосовує перехід від управління військами та зброєю до управління збройною боротьбою. Війна росії проти України свідчить, що в сучасній війні перемагає той, хто швидше сприймає нові технології та втілює їх у життя, бере на озброєння та практично впроваджує нові воєнні доктрини та концепції, які відповідають духу часу, і уможливлюють не лише використання нових технологій та ідей, а й добре знає, які з них як і коли використовувати. Високі технології сьогодні перетворюються в системоутворюючий фактор сучасної збройної боротьби. Вони дозволяють досягнути того нового етапу розвитку воєнного мистецтва-переходу від управління військами в ході збройної боротьби до управління конфліктом у цілому.

Ключові слова: *мережевоцентрична війна, гібридна війна, кільця Уордена, теорія Бойда.*

ВСТУП

Існування та розвиток сучасних ресурсів відбувається в тісному зв'язку з геополітичними та геостратегічними умовами і значною мірою залежить від міжнародних відносин. При цьому все більшого значення надається забезпеченню національній безпеці – стану захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз.

Серед багатьох факторів, що впливають на формування зовнішньої та внутрішньої політики держав, визначальна роль належить національним інтересам. Собою усвідомлюють на всіх рівнях суспільного життя, потреби народу країни у збережені та примноженні національних цінностей та національних багатств, в економічному процвітані та політичній стабільності суспільства, національні інтересам дістають своє відображення під час формування та досягнення національних цілей. Таким чином, виявляються пов'язаними національні інтереси і дії щодо їх досягнення. У міждержавних відносинах не тільки такі дії, а навіть і їх здійснення є об'єктами підвищеної уваги, ретельного вивчення та всебічної оцінки. Це особливо характерного для Європи, де переплетіння інтересів держав на перенаселеній та технологічно перенасиченій території спостерігається у найвищій мірі.

Крім того, обґрунтування національної стратегії воєнної безпеки є вважливим і відповідальним завданням. Стратегічне мислення є невід'ємним чинником ефективної політики. Як зазначив ще у 1927 році відомий теоретик воєнної науки О. Свечін: «Стратегія одна із найважливіших знарядь політики, політика й у час значною мірою має ґрунтувати свої розрахунки на військових можливостях дружніх і ворожих держав. Стратегія має заглядати у майбутнє і враховувати його у дуже широкій перспективі».

Аналіз сучасних військових конфліктів дає ключ до розуміння логіки дій учасників збройної боротьби в будь якій точці світу. Але цей арсенал передбачає не тільки вагомі матеріальні витрати, а й наявність політичній ваги держави, яка вирішу-