КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.2836
УДК 004

Дмитрук Яна Вікторівна
студентка 4 курсу факультету інформаційних технологій і математики
Волинський національний університет імені Лесі Українки, м. Луцьк,Україна
ORCID ID: 0000-0003-1734-9762
dmytruk.yana2018@vnu.edu.ua

Гришанович Тетяна Олександрівна
кандидат фіз.-мат. наук, доцент кафедри комп'ютерних наук та кібербезпеки
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID ID: 0000-0002-3595-6964
hryshanovych.tatiana@vnu.edu.ua

Глинчук Людмила Ярославівна
кандидат фіз.-мат. наук, доцент кафедри комп'ютерних наук та кібербезпеки
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID ID: 0000-0002-8943-9604
hlynchuk.ludmila@vnu.edu.ua

Жигаревич Оксана Костянтинівна
старший викладач кафедри комп'ютерних наук та кібербезпеки
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID ID: 0000-0002-1979-4168
zhyharevych.oksana@vnu.edu.ua

КІБЕРВІЙНА ЯК РІЗНОВИД ІНФОРМАЦІЙНИХ ВІЙН. ЗАХИСТ КІБЕРПРОСТОРУ УКРАЇНИ

Анотація. У роботі описано роль, яку відіграють фахівці з інформаційних технологій, зокрема кібербезпеки, в умовах війни в Україні. Окреслено поняття та рамки інформаційного фронту, виокремлено вклад технологів як у економіку, так і в сферу інформаційної війни. У статті описано перебіг та особливості ведення інформаційної війни на території нашої держави від 2014 року і до повномасштабного вторгнення російських військ на територію України. Описано внесок як вітчизняних так і іноземних фахівців з інформаційного захисту у перебіг цієї війни. Окреслено основні проблеми в інформаційному просторі, з якими доводиться зіштовхуватись в теперішніх умовах, а також наведено приклади допомоги в реаліях сьогоденної війни. У ході дослідження було з'ясовано, у яких саме напрямках рухаються вітчизняні ІТ-фахівці, яка їхня роль у нинішній ситуації, як задіюються іноземні структури та волонтери. Окрема роль відведена іноземним журналістів, які також воюють на інформаційному фронті, хоч і не є фахівцями з інформаційних технологій чи кіберзахисту. Таким чином, зрозуміло, що Україна виграє у інформаційній війні в першу чергу завдяки висвітленню правдивої інформації та її поширенні, а також завдяки активній протидії фейків. Також можна дійти до висновку, що інформаційний фронт є не менш важливим, ніж реальний, оскільки не лише послаблює ворога, а й ламає систему зсередини – руйнує логістику, виносить напоказ не найкращий бік ворога та здійснює інформування суспільства про реальний стан подій. Наразі українські та зарубіжні кібервійськові показують себе з найкращого боку: активно протидіють дезінформації та фейкам, вкладаються у економіку та нищать сайти, які ще функціонують. Перспектива нашого дослідження полягає у подальшому спостереженні за кіберфронтом. Важливо з'ясувати, яким чинному будуть розвиватися події, які іще застосунки (програмні, технічні) будуть розроблені для протидії агресору, чи будуть зроблені певні висновки зі сторони України. З нашої точки зору передбачається потужне покращення захисту усіх систем від можливості їх злому, підготовка кібервійськ на державному рівні та розробка нових рішень для захисту уже існуючого програмного забезпечення.

Ключові слова: інформаційна війна; кіберфронт; логістика; кіберзахист; кібербезпека.

ВСТУП

Постановка проблеми. Інформаційна війна виникла як форма ескалації інформаційних конфліктів. Переважно визначається, як латентний вплив інформації на індивідуальну, групову, масову свідомість за допомогою методів пропаганди, дезінформацію, маніпулювання з метою формування нових поглядів на соціально-політичну організацію суспільства. Інформаційно-технічна війна, або кібервійна, вимагає підготовки певного роду спеціалістів, як для захисту інформаційного простору, так і для ведення наступальних операцій. Дослідження роботи фахівців з інформаційних технологій кібербезпеки, надзвичайно важливе на сьогодні. Грунтовно досліджувалися теми, пов'язані із веденням бойових дій, які були на часі, роль ІТ-фахівців полягала виключно у виконанні поставленої задачі, тоді як інші країни наприклад США, Китай, Ізраїль, Німеччина активно готували спеціалістів кібервійськ, для здійснення атак на об'єкти критичної інфраструктури інших країн, кібершпигунів, які ведуть розвідувальну роботу [4, 33].

У час активного розвитку інформаційних технологій людству доводиться змінюватися, підлаштовуватися до нових правил. У такий спосіб разом із людьми видозмінюються й усі притаманні їм процеси, і війни у тому числі. Раніше фронт вибудовувався лише опираючись на тактику, воєнні технології та живу силу, сьогодні важливою складовою війни є інформаційна війна. Інформаційну війну науковці передусім характеризують як інформаційну діяльність, що здійснюється державою для ослаблення, знищення іншого політичного утворення, та як інформаційну боротьбу між конкурентами. Об'єктами, або ж, як це називають, театром війни, є інформаційний простір, інформаційні ресурси, системи управління, зв'язку, навігації, комп'ютерні мережі, радіоелектронні засоби тощо [3].

Інформаційні війни здійснюються заради досягнення певних завдань:

- донесення інформації;
- порушення логістики та роботи певних структур ворога;
- підрив морально-психологічного стану супротивника;
- дезінформація;
- зміна емоційного настрою;
- демонізація ворога або ж його залякування.

Актуальність роботи полягає у активному розширенні кіберфронту після повномасштабного вторгнення росії на територію України. Інформаційний фронт став однією з потужних сил, яка гарантувала українцям підтримку практично всього світу, а також неможливість ворога користуватися певними благами, які ще були доступні у країні-агресора.

Аналіз останніх досліджень і публікацій. Як уже було зазначено, тема не досліджувалася достатньо широко, а тому публікацій та інформації недостатньо, наразі процеси активізувалися. Було досліджено книги Когута Ю.І. [4] та іноземні публікації, зокрема, Вінода Аманда [14].

Мета статті полягає у дослідженні діяльності ІТ-спеціалістів в умовах воєнного стану, значення роботи кіберспільноти у реальній війни, а саме у розрізі інформаційної війни, розумінні того наскільки інформаційна війна визначає майбутню перемогу чи поразку країни, оскільки саме від представлення інформації, яка виноситься на загал і залежить формування думки більшості.

МЕТОДИКА ДОСЛІДЖЕННЯ

У ході дослідження використовувалася низка методів. Перш за все використовувалися емпіричні методи дослідження – спостереження, оскільки саме зараз відбувається переоцінка роботи IT-спеціалістів. Окрім цього, відбувався аналіз даних та проведення паралелей між українськими захисниками кіберпростору та уже давно відомими угрупуваннями хакерів з інших країн.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Під час дослідження увага приділялась активності українських кіберактивістів, (кіберкозаків), так і діяльності іноземних організацій. Найпотужнішим, хоч і найбільш примітивним засобом можна назвати масовані DDOS-атаки на більшість банків та установ у перші дні повномасштабного вторгнення. Такі дії призупиняли або ж повністю зупиняли роботу важливих інфраструктур. Створення хаосу дезорієнтує противника та виводить з ладу його логістичні центри та мережі [2].

Українські програмісти влаштовували DDoS-атаки проти російських пропагандистських ЗМІ, урядових сайтів та сайтів промислової сфери (авіакомпаній, онлайн-магазинів, ресурсів для створення ЕЦП, а також російського аналогу YouTube), Сбербанку та багато іншого. Українські IT-спеціалісти, працюють з програмою LOIK та disBalancer (особиста розробка українців, щоправда вона доступна лише для завантаження через архів), прописують команди на python та працюють з docker та DEATH BY 1000 NEEDLES (також українська розробка, яка доступна на Github).

Також було розроблено програму Liberator, а нещодавно додано до неї оновлення. Ця програма використовується для масованих атак на російські ресурси. Ці DDoS-атаки автоматизовані, тому користувачу нічого не потрібно робити, просто запустити Liberator на своєму ПК, а також встановити VPN чи використовувати Proxy Server. Звісно, краще, коли користувачі використовують віртуальні машини, проте це вже розраховано на більш досвідчених користувачів. Нова версія ввела функцію, яка дозволяє:

- самостійно налаштовувати цілі;
- можливість Ddos-ити декілька ресурсів;
- вказувати кількість потоків.

«Liberator 0.2.0 – це продовження нашої битви з росіянами. Щоб посилити атаки, ми постійно вдосконалюємо програмне забезпечення. Мультитаргетинг у Liberator дозволяє зробити атакувальний процес набагато сильнішим та ефективнішим. Він надає дисбалансерам нові можливості», – зазначили розробники на сайті [9].

Зламали українські хакери і мережу, яка була заборонена на території України – «Вконтакте». Окрім цього, було злито листування Солохи Валерія, співробітника ФСБ росії, з колаборантами з Херсонської області – Кирилом Стремоусовим та Віктором Яценко. У ході обміну повідомлень чоловіки розповідали про настрої на тимчасово окупованих територіях, обмінювалися думками про придушення проукраїнських сил та шляхами дискредитування ЗСУ, повідомлялося про переміщення української військової техніки. Також активно поширювалася проросійська пропаганда, зокрема про створення так званої «Херсонської Народної Республіки» [10].

Також була організована масована кібератака на інтернет-провайдера, який функціонує у нині окупованому Криму. Провайдером виявилася компанія «Міранда-медіа». При цьому інтернет не просто не працював, при пошуковому запиті у системах замість звичного опису були заклики про те, що « Крим – Україна» і що «ми вас

[кримчан] любимо», а замість назви сайту була назва телеграм-каналу українських кіберкозаків. Результати цієї атаки на діяльність самої мережі невідомі [6].

Згідно статистики, частка фахівців, які долучилися до захисту кіберфронту сягає 5% з усіх фахівців галузі, проте деякі компанії повністю змінили свою кваліфікацію та практично всі їх працівники долучились до захисту кіберпростору України. Важливо зазначити, що більшість IT-спеціалістів продовжують сплачувати податки, підтримуючи таким чином іще й економічний фронт [11].

Найгучнішим нападом можна вважати атаку на ЄДАІС – Єдину державну автоматизовану інформаційну систему. Проте проблеми виникли не так з самою системою, як з тим, що було спричинено проблеми з перевезенням алкоголю, які налагоджувалися цією системою. Видання Profibeer повідомило, що відповідальними за масовані атаки є українці, що продовжать атаки на цей ресурс та дочірні до нього компанії. Через атаку алкогольні напої припинили постачатися на територію рф [8].

Зупинено роботу аналогу YouTube російського виробництва. З 8 на 9 травня 2022 року система була масово атакована та було пошкоджено усю систему, як бази даних, так і систему документообігу [7].

Проте неправильно вважати, що хакерство в Україні набрало розвитку лише зараз, як і вважати, що війна розпочалася лише зараз (тому доцільно брати до уваги відрізок часу з 2014 року). Після анексії Криму у 2014 році було організовано український кібер-альянс з активістів та усіх небайдужих. Займалися вони тим же, чим зараз займаються кіберкозаки – атаки на російські сайти та спричинення витоків даних. Була інформація, що саме вони відповідальні за злиття бази даних з телефонами та електронними поштами сепаратистів.

Найбільшим досягнення хактивістів (хакерів-активістів) можна вважати злом та розповсюдження електронної пошти Владислава Суркова, близького радника Путіна щодо конфлікту на сході України, це сталося у 2016 році. Витік інформації показав спроби Суркова дестабілізувати Україну, підірвати її уряд та організувати вибори деяких політиків-сепаратистів. Ці дані стали вагомим доказом підривної діяльності, яку москва раніше заперечувала [16].

Важливим внеском у інформаційно-технічну війну є спростування фейків та донесення правдивої інформації. Цим займається волонтерське угрупування людей, які власноруч перевіряють новини на наявність у них фейків і відповідно спростовують новину. Сайт Stopfake.org, який націлений на перевірку фейків, був запущений у 2014 році завдяки активістам з Могилянської школи журналістики. На сьогодні кількість залучених людей зростає і вони поширюють інформацію вже 13 мовами: російською, англійською, українською, іспанською, румунською, болгарською, французькою, італійською, голландською, чеською, сербською, німецькою та польською мовами. Варто відзначити, що сфера стосується IT-спеціалістів, оскільки іноді доводиться перевіряти чи не піддавалися фото чи відео видозмінам, а не лише шукати інформацію та перекладати її [1].

Україна вперше отримала дві важливі нагороди у сфері кібербезпеки на CYBERSEC European Cybersecurity Forum 17 травня 2022 р. Зокрема за зусилля та успіхи у захисті цифрового простору України та захист цифрових кордонів демократичного світу. Також було відзначено, що Україна героїчно протистоїть російській агресії та захищає цифровий фронт демократичного світу, окремо було відзначено Михайла Федорова – міністра цифрової трансформації України [13].

Михайло Федоров наймолодший міністр у історії держави України. Перспективний, надзвичайно розумний керівник, очолив на інформаційному фронті кіберзахист. Використовуючи Twitter-аккаунт для тиску на Apple, Facebook та інші

компанії для будування «цифрової блокади» проти рф, його тактика перетворюється на потужний закулісний наступ. Міністерство цифрової трансформації зробила розсилку повідомлень із закликом виходу з російського ринку, надіслано понад 4000 запитів компаніям, урядам та іншим організаціям, кожен із яких особисто підписав М. А. Федоров. За його словами, підтримується зв'язок із тисячами керівників невеликих підприємств, оскільки американські компанії вживають заходів для обмеження бізнесу в рф на тлі суспільного тиску та санкцій. Команда Федорова зосереджується на малоймовірному союзнику: Великих китайських компаніях, таких як DJI та Alipay. Михайло Федоров 26 лютого 2022р. звернувся до Ілона Маскам із проханням забезпечити Україну доступом до супутникового Інтернету. Згодом до України доставили тисячі супутників Starlink, для підключення до Інтернет – мережі, щоб відновити зв'язок на сході [18].

Кіберпростір відзначається тим, що для нього не існує державних кордонів, об'єднує географічні доменні зони, інтернет простір знаходяться у одному інформаційному середовищі. Важливий внесок у перебіг кібервійни зробило об'єднання хакерів Anonymous. 25 лютого 2022 року акаунти Twitter, пов'язані з Anonymous, оголосили, що вони розпочали «кібероперацію» проти російської федерації у помсту за вторгнення в Україну. Пізніше група тимчасово вимкнула ряд веб-сайтів, перш за все це сайт кремля (http://kremlin.ru) та сайт (російського міністерства захисту (http://mil.ru). Також хакери атакували сайт російської пропагандистської станції RT News (http://rt.com).

Варто відзначити, що Anonymous не обмежилися звичайними атаками на сайти, декілька разів ставався потужний витік інформації, так хакери злили базу даних сайту Міноборони росії (mil[.]ru). Було злито близько 200 ГБ електронних листів від білоруського виробника зброї Tetraedr. Компанія надала володимиру путіну матеріально-технічну підтримку, таким чином хакери оголосили війну не лише путіну, а й усім, хто причетний до ведення війни проти України. Блокування сайту чеченської республіки (http://chechnya.gov.ru), теж завдяки роботі Anonymous.

Хакерська група GNG разом з Anonymous злила бази даних СберБАНКу росії на підтримку українського народу. Конфіденційна інформація Газпрому опинилися у відкритому доступі. Також спричинили витік інформації та електронних листів на більш ніж 200 ГБ, розмістивши ці дані на хмарному сховищі MEGA (через декілька днів їхній обліковий запис був заблокований і до даних не можна було достукатися). 29 березня 2022 року стався витік файлів двох російських компаній «МашОйл» і «РостПроект» на 112 ГБ даних. Anonymous програмно взламали російські телеканали, представляли через них українську музику, нецензурні новини, правду про перебіг подій в Україні, лунав у ефірі гімн України. Anonymous висвітлювала події щодо боротьби проти рф у себе на аккаунті в Twitter. Сайти російських пропагандистських ЗМІ ТАСС, «Известия», «Фонтака», РБК і «Коммерсантъ» також були зламані Anonymous.

Також організація Anonymous поширила базу даних з інформацією про 120 000 російських військових, які брали участь у вторгненні в Україну. Посилання на злам розміщено в офіційному твітері Anonymous. Проте основну частину інформації дістали саме українські хакери з E_N_I_G_M_A. Звісно, відбувалося доповнення інформації, яку вдалося дістати у ході власних розслідувань. Вперше база була опублікована 25 лютого 2022 року з даними про 100 000 військових, проте у цій базі даних міститься інформація, яка була актуальна на 2018 рік, тобто не всі військовослужбовці у ній можуть бути вказані, і не всі можуть брати участь у військових діях станом на 2022 рік.» [12]. Окрім того, було створено веб-сайт https://www.1920.in/, який розроблений для того, щоб автоматично телефонувати чи робити розсилку рандомно обраному користувачу з рф,

щоб вони знали правду. 4 квітня 2022 року DDoSecrets опублікував понад 900 000 листів від всеросійської державної телерадіокомпанії (ВГТРК), які були зламані анонімом NB65 [17].

Хакери заявили, що злили 15 ГБ даних, які пов'язані з діяльністю російської православної церкви, проте перевірити правдивість їх висловлювань не є можливим, оскільки доступ до цих даних вони надають лише журналістам та дослідникам [5].

Важливим кроком згадати – участь звичайних іноземців у інформаційній війні на стороні України. Мова йде не лише про іноземних кореспондентів, які доносять правду, а й про активістів, які доєднались до української кіберспільноти (після того, як дізналися про наявність іноземців у телеграм-каналі ІТ-армії почали дублювати всю інформацію англійською), підписали понад 300 000 людей, у тому числі й з-за кордону. Західні чиновники заявили, що вони «наполегливо не рекомендують» приєднуватися до групи та брати участь у хакерській діяльності проти рф. «Ми не будемо заохочувати злочинність будь-яким способом, шляхом чи формою», «Ми б рішуче не заохочували людей брати участь у таких видах діяльності».

Кіберзахист України мав особливий успіх із розподіленими атаками відмови в обслуговуванні (DDoS), під час яких веб-сайти стають недоступними через бомбардування трафіком. Таким чином об'єктом атак стали російські урядові вебсайти, зокрема кремль і дума, а також державна служба новин Russia Today. Anonymous, хакерська група, взяла на себе відповідальність за DDoS-атаки. На думку експертів, приєднання до українських кібератак із США чи Великобританії може порушити закон у цих країнах, наприклад, Закон «Про комп'ютерне шахрайство та зловживання» в США та закон «Про зловживання комп'ютерами» у Великобританії. «Це не тільки може бути незаконним, але й з'являється ризик, що це може зіграти на руку путіну, дозволяючи йому говорити про «атаки із заходу», — сказав Алан Вудворд, професор кібербезпеки в Університеті Суррея. Зважаючи на такі занепокоєння зі сторони представників уряду, у кібервійськах задіяно багато іноземців, і самі представники влади відмічають, що були все ж задіяні деякі механізми допомоги. «За лаштунками [були] … масові зусилля міжнародного уряду для підтримки наших українських союзників на інформаційному просторі» [17].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході дослідження було з'ясовано у яких саме напрямках рухаються наші ІТ-спеціалісти, яка їхня роль у нинішній ситуації, як працюють іноземні структури та волонтери, не варто також забувати про іноземних журналістів, які також воюють на інформаційному фронті, хоч і не є ІТ-спеціалістами. Таким чином, зрозуміло, що Україна перемагає у інформаційній війні в першу чергу завдяки висвітленню інформації та її поширенні, а також активній протидії фейків та дестабілізації ворога. Усе це справа рук кіберактивістів. Завдяки потужному інформаційному фронту та звісно протистоянню на реальному полі битви ми досягнули підтримки від майже цілого світу: якби не існувало впевненої протидії на якомусь із цих напрямків, то війна швидше за все була б програна. Підсумовуючи все вищесказане, можна дійти до висновку, що інформаційний фронт є не менш важливим, ніж реальний, оскільки не лише послаблює ворога, а й ламає систему зсередини – руйнує логістику, виносить напоказ не найкращу сторону ворога та здійснює інформування суспільства про реальний стан подій. У ході війни українські та зарубіжні кібервійськові показують себе з найкращої сторони: активно протидіють дезінформації та фейкам, вкладаються у економіку та нищать сайти, які ще функціонують.

Перспектива полягає у подальшому спостереженні за кіберфронтом, як будуть розвиватися події, які застосунки розроблять IT-спеціалісти для протидії агресору, чи будуть зроблені певні висновки зі сторони України. З нашої точки зору передбачається потужне покращення захисту усіх систем від можливості їх взлому, підготовка кібервійськ на державному рівні та розробка нових застосунків для захисту уже існуючих програм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Головна*. StopFake. https://www.stopfake.org/uk/golovna/
2 *Економічна правда. IT у війні: як працює індустрія.* Економічна правда. https://www.epravda.com.ua/columns/2022/03/22/684494/
3 *Інформаційна війна.* Енциклопедія Сучасної України. https://esu.com.ua/search_articles.php?id=12460.
4 Когут, Ю. І. (2019). *Кібервійна та безпека об'єктів критичної інфраструктури*. Консалтинг. Компанія «Сідкон».
5 *Українська правда. Хакери злили 15 ГБ даних, викрадених у РПЦ – Anonymous.* Українська правда. https://www.pravda.com.ua/news/2022/04/2/7336517/.
6 *Українські хакери атакували найбільшого інтернет-провайдера Криму*. Новини Черкас. https://cherkasy24.info/24101-ukrayinsk-hakeri-atakuvali-nayblshogo-nternet-provaydera-krimu.html.
7 *Українські хакери розповіли, як "поклали" найбільший російський відеохостинг Rutube.* https://www.unian.ua/techno/ukrajinski-hakeri-rozpovili-yak-poklali-naybilshiy-rosiyskiy-videohosting-rutube-11826486.html.
8 *ФОКУС "Не зможуть користуватися кілька днів": DDoS-атаки порушили постачання алкоголю в РФ*. ФОКУС. https://focus.ua/uk/digital/514723-ne-smogut-polzovatsya-neskolko-dney-ddos-ataki-narushili-postavki-alkogolya-v-rf.
9 *ФОКУС Р. Українські хакери покращили кіберзброю проти Росії: атакувати може кожен*. ФОКУС. https://focus.ua/uk/digital/515246-ukrainskie-hakery-uluchshili-kiberoruzhie-protiv-rossii-kiberatakovat-mozhet-kazhdyy.
10 *Хакери оприлюднили переписку проросійських колаборантів з кураторами з ФСБ.* Gazeta.ua. https://gazeta.ua/articles/life/_hakeri-oprilyudnili-perepisku-prorosijskih-kolaborantiv-z-kuratorami-z-fsb/1074964.
11 *Як IT індустрія наближає перемогу України.* 24 Канал. https://tech.24tv.ua/yak-it-industriya-nablizhaye-peremogu-ukrayini_n1919788.
12 *Anonymous поширив базу даних про 120 000 військових РФ. Її злили українські хакери.* AIN.UA. https://ain.ua/2022/04/04/anonymous-poshyryv-bazu-danyh-rosijskyh-vijskovyh/.
13 *European Cybersecurity Forum - CYBERSEC. 📣 The 2022 European CYBERSEC Award goes to Vice Prime Minister and Minister of Digital Transformation of Ukraine, Mr Mykhailo.* Twitter. https://twitter.com/CYBERSECEU/status/1526472712297889796.
14 Malik, V. P. (2006). *Defence planning: Problems and prospects*. Manas Publications.
15 Milmo, D. (2022, 18 березня). *Amateur hackers warned against joining Ukraine's 'IT army'*. the Guardian. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
16 Shore, J. (2022, 11 квітня). *Don't Underestimate Ukraine's Volunteer Hackers*. Foreign Policy. https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/
17 Thalen, M. *Hackers steal 900K emails from Russia's largest state-owned media corporation.* The Daily Dot. https://www.dailydot.com/debug/hackers-vgtrk-920k-emails-anonymous-russia/
18 Zakrzewski, C. (2022, 30 березня). *4,000 letters and four hours of sleep: Ukrainian leader wages digital war*. Washington Post. https://www.washingtonpost.com/technology/2022/03/30/mykhailo-fedorov-ukraine-digital-front/
19 *Zn.ua. Атаки українських хакерів призвели до припинення роботи пивзаводів у Росії.* Зеркало недели | Дзеркало тижня | Mirror Weekly. https://zn.ua/ukr/TECHNOLOGIES/ataki-ukrajinskikh-khakeriv-prizveli-do-pripinennja-roboti-pivzavodiv-u-rosiji.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Yana V. Dmytruk
the 4th year student of the faculty of information technologies and mathematics,
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID ID: 0000-0003-1734-9762
dmytruk.yana2018@vnu.edu.ua

Tetiana O. Hryshanovych
PhD, Associate Professor at the Department of Computer Science and Cybersecurity
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID ID: 0000-0002-3595-6964
hryshanovych.tatiana@vnu.edu.ua

Liudmyla Y. Hlynchuk
Ph.D, Associate Professor at the Department of Computer Science and Cybersecurity
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID ID: 0000-0002-8943-9604
hlynchuk.ludmila@vnu.edu.ua

Oksana K. Zhyharevych
Seniot Lecturer at the Department of Computer Science and Cybersecurity
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID ID: 0000-0002-1979-4168
zhyharevych.oksana@vnu.edu.ua

CYBERWAR AS A VARIETY OF INFORMATION WARS. UKRAINIAN CYBER SPACE PROTECTION

Abstract. The paper describes the role played by information technologies, including cybersecurity, specialists, during the war in Ukraine. The concept and framework of the information front are outlined, the contribution of technologists to both the economy and the field of information warfare is highlighted. The article describes the course and circumstances of the information war on the territory of our state from 2014 until the full-scale invasion of Russian troops on the territory of Ukraine. The contribution of both domestic and foreign information protection specialists to the course of this war is described. The main problems in the information space that we have to face in the current conditions are outlined, as well as examples of assistance in the realities of today's war. The study found out in which directions domestic IT specialists are moving, what is their role in the current situation, how are foreign structures and volunteers involved. The separate role is given to foreign journalists who are also fighting on the information front, but they are not specialists in information technology or cybersecurity. Thus, it is clear that Ukraine will win in the information war primarily due to the coverage of true information and its dissemination, as well as due to the active opposition to fakes. It can also be concluded that the information front is no less important than the real one, as it not only weakens the enemy, but also breaks the system from within - destroys logistics, flaunts not the best side of the enemy and informs society about the real state of events. Currently, Ukrainian and foreign cyber troops are doing their best: actively opposing disinformation and fakes, investing in the economy and destroying sites that are still operational. The perspective of our study is to further monitor the cyberfront. It is important to find out how events will run, what other applications (software, technical) will be developed to counter the aggressor, whether certain conclusions will be drawn from Ukraine. From our point of view, there is a strong improvement in the protection of all systems from the possibility of hacking, training of cyber troops at the state level and the development of new solutions to protect existing software.

Keywords: information war; cyberfront; logistics; cyber security; cybersecurity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 *Home*. StopFake. https://www.stopfake.org/uk/golovna/.

2 *Economic truth. IT in the war: how the industry works.* Economic truth. https://www.althoughda.com.ua/columns/2022/03/22/684494/.
3 *Information war.* Encyclopedia of Modern Ukraine. https://esu.com.ua/search_articles.php?id=12460.
4 Kohut, Yu. I. (2019). Kiberviina ta bezpeka obiektiv krytychnoi infrastruktury. Konsaltynh. Kompaniia «Sidkon».
5 *Ukrainian truth. Hackers leaked 15 GB of data stolen from the ROC - Anonymous.* Ukrainian Pravda. https://www.pravda.com.ua/news/2022/04/2/7336517/.
6 *Ukrainian hackers attacked the largest Internet provider in Crimea*. News Cherkasy. https://cherkasy24.info/24101-ukrayinsk-hakeri-atakuvali-nayblshogo-nternet-provaydera-krimu.html.
7 *Ukrainian hackers told how they "put" the largest Russian video hosting Rutube*. https://www.unian.ua/techno/ukrainski-hakeri-rozpovili-yak-poklali-naybilshiy-rosiyskiy-videohosting-rutube-11826486.html
8 *FOCUS "Can not use a few days": DDoS-attacks disrupted the supply of alcohol in Russia.* FOCUS. https://focus.ua/uk/digital/514723-ne-smogut-polzovatsya-neskolko-dney-ddos-ataki-narushili-postavki-alkogolya-v-rf
9 *FOCUS R. Ukrainian hackers have improved cyber weapons against Russia: anyone can attack.* FOCUS. https://focus.ua/uk/digital/515246-ukrainskie-hakery-uluchshili-kiberoruzhie-protiv-rossii-kiberatakovat-mozhet-kazhdyy
10 *Hackers have published correspondence between pro-Russian collaborators and curators from the FSB.* Gazeta.ua. https://gazeta.ua/articles/life/_hakeri-oprilyudnili-perepisku-prorosijskih-kolaborantiv-z-kuratorami-z-fsb/1074964
11 *How the IT industry is approaching Ukraine's victory.* 24 Channel. https://tech.24tv.ua/yak-it-industriya-nablizhaye-peremogu-ukrayini_n1919788.
12 *Anonymous has distributed a database of 120,000 Russian military. She was merged by Ukrainian hackers*. AIN.UA. https://ain.ua/2022/04/04/anonymous-poshyryv-bazu-danyh-rosijskyh-vijskovyh/.
13 *European Cybersecurity Forum - CYBERSEC. 📣 The 2022 European CYBERSEC Award goes to Vice Prime Minister and Minister of Digital Transformation of Ukraine, Mr Mykhailo.* Twitter. https://twitter.com/CYBERSECEU/status/1526472712297889796.
14 Malik, V. P. (2006). *Defence planning: Problems and prospects*. Manas Publications.
15 Milmo, D. (2022, 18 березня). *Amateur hackers warned against joining Ukraine's 'IT army'*. the Guardian. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
16 Shore, J. (2022, 11 квітня). *Don't Underestimate Ukraine's Volunteer Hackers*. Foreign Policy. https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/
17 Thalen, M. *Hackers steal 900K emails from Russia's largest state-owned media corporation.* The Daily Dot. https://www.dailydot.com/debug/hackers-vgtrk-920k-emails-anonymous-russia/
18 Zakrzewski, C. (2022, 30 березня). *4,000 letters and four hours of sleep: Ukrainian leader wages digital war*. Washington Post. https://www.washingtonpost.com/technology/2022/03/30/mykhailo-fedorov-ukraine-digital-front/.
19 *Zn.ua. Attacks by Ukrainian hackers have led to the closure of breweries in Russia.* Mirror of the Week Mirror of the week | Mirror Weekly. https://zn.ua/ukr/TECHNOLOGIES/ataki-ukrajinskikh-khakeriv-prizveli-do-pripinennja-roboti-pivzavodiv-u-rosiji.html