КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4(16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.3744
УДК 004

Мальцева Ірина Робертівна
Старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-6073-4637
irenagold2402@gmail.com

Черниш Юлія Олександрівна
Старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-6626-5656
kobernikoi@ukr.net

Штонда Роман Михайлович
Начальник науково-дослідного відділу
Військовий інститут інформаційно-телекомунікаційних технологій імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-5986-0847
shtonda1982@ukr.net

АНАЛІЗ ДЕЯКИХ КІБЕРЗАГРОЗ В УМОВАХ ВІЙНИ

Анотація. У даній статті досліджені найвідоміші та найгучніші кіберзагрози, які були здійснені по відношенню до держави під час вторгнення рф. Ми проаналізували також і закони, що були прийняті під час воєнних дій на території нашої держави. Вони суттєво вплинули на захист від подальших загроз для всієї системи. Проблематика руйнівних та нищівних кібератак росії перед вторгненням в нашу країну доводить, що кібератаки відіграють важливу та стратегічну роль в сучасному світі та війні, незважаючи на те, чи відомо про це громадськості. Ця загроза для нас є постійною і вона не стоїть на місці та розвивається. Кібератаки завдають чималих проблем нашій системі та інфраструктурі з парадоксальними наслідками. Безпека України суттєво залежить від забезпечення кібербезпеки. На цьому варто не тільки акцентувати увагу, а й навіть докласти максимальних зусиль. Технічний прогрес зростатиме, а за нею і дана залежність в кіберпросторі. Зазначимо, що законодавче регулювання відносин теж має свої потреби, щодо постійного оновлення та супроводження стрімкого розвитку технологічних процесів.

Ключові слова: кібератаки, кіберзагрози, кіберзахист, кіберпростір

ВСТУП

Неодмінними атрибутами сучасних глобалізаційних процесів є стрімкий науково-технічний прогрес: цифровізація суспільних відносин, вихід людства у кіберпростір, проникнення віртуального світу в усі сфери життєдіяльності. В кінцевому варіанті все вищесказане формує нескінченні та різноманітні можливості сучасного розвитку інформаційного суспільства. Проте поруч із розвитком прогресуючих складових, технологічний прогрес стимулює появу нових викликів та окремих загроз, зокрема і щодо балансу безпечних та надійних інтересів на національних та міжнародних рівнях. За останні роки загрози порушення інтересів людей, самої держави й у цілому людства в кіберпросторі перейшли із потенційних та гіпотетичних на цілком реальні. Тож протистояння їх поширенню стало пріоритетним завданням на національному рівні урядів та міжнародної спільноти.

Постановка проблеми. Найактуальнішою загрозою та проблемою є саме кібератаки, пов’язані з ситуацією на території нашої держави. Повномасштабне

вторгнення російських військ на територію нашої країни супроводжується сильною агресією у кіберпросторі. Нашій країні довелось зіткнулися з новим та серйозним рівнем кіберзагроз.

Аналіз останнніх досліджень і публікацій. На даний час, та в тих умовах, в яких перебуває наше суспільство, ми здійснили комплексне дослідження адміністративно-правових основ кібербезпеки, на основі аналізу чинного національного та міжнародного законодавства, практики його застосування та реалізації в умовах війни, а також переглянули найбільш гучні та відомі кіберзагрози під час воєнної агресії рф [1].

Мета статті. Метою даної статті є можливість обговорення цих проблем, їх аналізу, пошуку рішень для забезпечення кібербезпеки та шляхів захисту кіберпростору (інформаційного простору і т.п.) в умовах воєнних дій на території нашої сильної та незалежної країни.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В наш час вплив в кіберпросторі може з неймовірною швидкістю розгорнути ситуацію в суспільстві в напрямі, потрібному нашому ворогу «Рис. 1» [2].

Рис.1 Кіберзагроза є важливим сигналом світу

З 2018 року при Службі безпеки України працює Ситуаційний центр забезпечення кібербезпеки. Ця структура створювалася за допомогою Північноатлантичного альянсу - технічне обладнання та програмне забезпечення для роботи Центру було надано в рамках виконання першого етапу Угоди про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки. На базі Ситуаційного центру функціонує система управління подіями інформаційної безпеки, яка моніторить події у режимі реального часу і дозволяє аналізувати стан інформаційної безпеки. І це дає змогу оперативно виявляти, реагувати та попереджувати загрози в національному кіберпросторі. В середньому, за статистикою Держслужби спеціального зв'язку та захисту інформації (Держспецзв'язку), щонеділі в Україні блокувалось до 50 тисяч кібератак на державні інформаційні ресурси [3].

Як показують останні події, війна в інформаційному просторі завдає не меншої шкоди, аніж війна на полі бою. І це без жодних перебільшень. Розуміючи це все, у перші два місяці воєнних дій парламент оперативно та одноголосно оптимізував кримінальне та кримінально-процесуальне законодавство. Удосконалив також підстави та самі процесуальні механізми щодо притягнення до кримінальної відповідальності всіх кіберзлочинців. Зміни зосереджено у двох даних законах:

1. «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 року;

2. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 року.

Якщо другий прийнято давно, то закон № 2149-IX набрав чинності досить недавно - тільки 3 квітня 2022 року [**Error! Reference source not found.**].

Від самого початку війни стало відомо про величезну кількість кібератак на українські ресурси. Напад російських хакерів на Україну розпочався буквально за кілька хвилин до повномасштабного вторгнення армії. За даними агентства Reuters, США, Великобританія та Європейський Союз офіційно звинуватили рф у великомасштабному кібернападі, який порушив роботу супутникового інтернет-сервісу Viasat за годину до початку війни, 24 лютого 2022 року. Це спричинило знищення «десятків тисяч» супутникових терміналів [5]. Активно зазначається що, дана атака торкнулася також європейських інтернет-користувачів та деяких вітрових електростанцій «Рис. 2». А ще під хвилю потрапили українські військові та декілька сотень цивільних клієнтів.

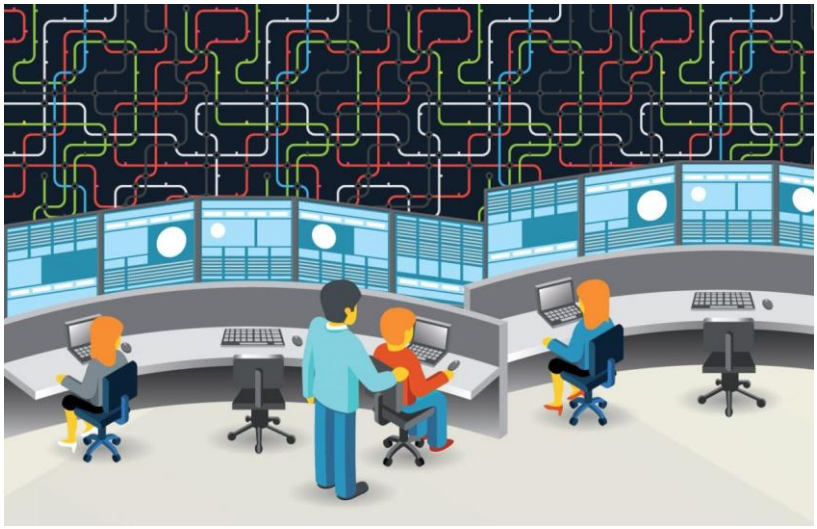

Рис.2 Протидія кібератакам потребує зусиль

За конкретними даними MIT Technology Review напад російських хакерів на платформу Viasat це — найбільший відомий та болючий злом під час війни. Про це наголошував Хуан Андрес Герреро-Сааде. Це відомий дослідник кіберзагроз із SentinelOne. Даний злом, один із перших живих прикладів того, як кібератаки можуть бути направлені та конкретно розраховані за часом для посилення ворожих збройних сил на нашій землі, шляхом порушень та навіть цілковитого знищення розвинутих технологій. В ході цієї кібератаки, 24 лютого 2022 року запустили дуже шкідливе програмне забезпечення AcidRain. Воно стерло всі дані модемів та маршрутизаторів Viasat, і в результаті чого вони всі відключилися. Таким чином на знищення пішли тисячі терміналів. Попереднє програмне забезпечення російських хакерів було вузько спрямованим та сильно шкідливим для системи. Та все ж AcidRaid є скоріше універсальною зброєю.

ISSN 2663 - 4023

Не так давно Держспецзв'язок повідомив про масове отримання українськими користувачами нового напливу небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання шахраями повного контролю над вашим пристроєм, а точніше ноутбуками та комп'ютерами, що загрожує крадіжкою та пошкодженнями комп'ютерних даних.

Наступним потрібно згадати незграбну спробу атаки хакерського угруповування Strontium. Вони намагалися зосередити всі свої зусилля на отримані доступу до всіх комп'ютерних мереж в Україні, США та ЄС. Цими нищівними діями вони планували забезпечити підтримку фізичного вторгнення росії в Україну на тактичному рівні, викрасти та знешкодити всю конфіденційну інформацію.

Є інформація, що 23 березня 2022 року ворог намагався здійснити потужну кібератаку на наші державні установи з використанням шкідливих та мало знайомих нашій системі програм, одна з них Cobalt Strike Beacon. Вона сильно та безповоротно вражає всю систему у випадку її відкриття.

4 квітня 2022 року Держспецзв'язок дав екстрене попередження про масове розповсюдження електронних листів, що носило назву «Військові злочинці РФ.htm». Їхнє відкриття призводить до того, що хакери отримують віддалений доступ до комп'ютерів жертв.

Постійно під прицілами знаходяться об'єкти критичної інфраструктури. Відомий український провайдер Укртелеком потрапив під потужну атаку 28 березня 2022 року, під час якої зловмисники намагалися зламати та проаналізувати як влаштована IT-інфраструктура. В їхні плани входило вивести з ладу обладнання та різні сервіси. Також вони намагалися отримати контроль над мережею та обладнанням даної компанії.

За оцінками Канади, за цими інцидентами стоять досвідчені російські військові. Російське незаконне вторгнення до України, її шкідлива кібернетична діяльність та обурливі дезінформації кампанії – неприйнятні та мусять припинитися [6]. Зазначається що, урядовці підкреслили, що Канада "ділиться цінною та унікальною розвідувальною інформацією, яка стосується кіберзагроз та надає цінну кібердопомогу Україні. Вона явно намагається зміцнити оборону нашої країни проти російського невиправданого, несправедливого та незаконного вторгнення".

Це приклади лише масованих атак «Рис. 3». Ймовірно, про атаки менших масштабів та окремі випадки персональних зламів просто мало що відомо, і сильно не інформують у суспільстві[7].

Рис.3 Загроза масованих атак все дедалі частішає

Також важливим фактом є те, що ще до початку воєнних дій, після славнозвісної кібератаки 14 січня 2021 року на сайти державних органів влади, відчувалася конкретна необхідність запровадження невідкладних змін на рівні українського законодавства, для узаконення процедури Bug Bounty (залучення зовнішніх фахівців до пошуку помилок і вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо) [**Error! Reference source not found.**]. На сьогодні ІТ-спільнота вже легко зможе легально тестувати всі необхідні державні інформаційні системи на наявність вразливого місця, а сама держава отримає невідкладні інструменти для значного підвищення ступеня захисту саме таких систем.

Слід зазначити що, від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові, так звана «КіберАрмія». Звичайні люди, поряд із професіоналами сфери ІТ, наносять нищівний удар атакуючи ворога у кіберпросторі, завдають йому збитків та зривають плани.

Кожному під час воєнного стану варто звернути увагу на дані точки контролю:

1. Старатися вивчати та активно аналізувати слабкі місця вашого кіберзахисту, щоб щоденно укріплювати їх. Хакери завжди здійснюють багато розвідувальних операцій в Україні. Таким чином вони знаходять найслабші місця в захисті наших компаній та скориставшись цим атакують, б'ючи по них. Ніколи не існувало та не існує на 100% захищених систем. Варто зазначити, чим менше вартуватиме шахраям злом будь-якої системи, то вищою буде їхня мотивація.

2. Тим, хто перебуває в зоні кіберризику, варто безупинно слідкувати за відповідними повідомленнями на різних офіційних ресурсах Держспецзв'язку та CERT-UA. Ці органи першими публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати їхні ризики [9].

3. Потрібно завжди пам'ятати про безпеку системи, яка залежить конкретно та абсолютно точно від кожного працівника. Хакери здатні напасти на компанію або ж установу і через робітників різних фірм та установ, викравши їхні дані. В особливій небезпеці знаходяться – військові, а також всі державні діячі. Ці категорії людей мають абсолютно точно звикнути до кібергігієни та прийняти її за норму повсякденного життя, щоб не боротися з важкими наслідками в разі атак.

4. Для тих хакерів, хто проводить небезпечні та щоденні кібератаки на ворогів та займається багхантингом з чітким планом удосконалення та зміцнення української кібербезпеки в умовах воєнного часу, задля повного уникнення невирішених проблем із службою правоохоронних органів потрібно бути повністю готовими довести відповідність своєї діяльності інтересам України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Слід зафіксувати, що мега ефективна та кваліфікована протидія загрозам національній безпеці у кіберсфері стає реальною тільки за певної умови щодо комплексного використання всього арсеналу правових засобів для найкращого забезпечення кібербезпеки. Це стосується пунктів , які діють за всіма структурованими елементами державного управління та на всіх етапах обігу інформації. Можемо сміливо стверджувати, що найкращий ефект полягає у повній взаємодії суб'єктів забезпечення кібербезпеки України. Цього можливо досягнути шляхом використання цілісних та дієвих системних механізмів, адміністративно-правових методик та різноманітних засобів, завдяки яким здійснюються реалізації державної політики у сфері повного забезпечення кібербезпеки, як складових елементу національної безпеки України.

Державні органи, урядові організації разом з українськими компаніями з кібербезпеки і найголовнішими світовими виробниками рішень запровадили ешелонований кіберзахист для нашої рідної держави та бізнесу в цілому. Та все ж потрібно й надалі докладати зусиль, аналізувати ситуації та шукати рішення. Ми маємо бути сильними, стійкими до всіх зовнішніх ризиків та негараздів, продовжувати компетентно та рішуче надавати послуги всім громадянам, забезпечувати тривале функціонування бізнесу та й в цілому всієї економіки країни.

Боремося з кібертерором разом! Разом до перемоги! Слава Україні!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Веселова, Л. Ю. (2021). *Адміністративно-правові основи кібербезпеки в умовах гібридної війни* [Дис. д-ра]. http://oduvs.edu.ua/wp-content/uploads/2016/06/Disertatsiya_Veselovoi_L.YU..pdf.

2 *Що таке фішинг і як від нього захиститися?* https://www.tecnoseguro.com/media/k2/items/cache/a7ac92c0202d08b485ecb09c07ac6372_XL.jpg.

3 *Безпека у кіберпросторі.* Головна. https://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1126-bezpeka-u-kiberprostori.

4 https://jurliga.ligazakon.net/. (2022, 13 квітня). *Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX | ЮРЛІГА*. ЮРЛІГА. https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix

5 *Війна росії проти україни почалася з кібернападу на супутники. за годину до вторгнення були знищені «десятки тисяч» терміналів Viasat - itc.ua.* ITC.ua. https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/

6 *Канада надає україні розвіддані про кіберзагрози – tokar.ua.* Tokar.ua. https://tokar.ua/read/48906

7 *Як малому бізнесу захистити себе від кіберзагроз.* https://businessviews.com.ua/files/news_tape/images/20/40/picture_jak-malomu-biznesu-z_2040_s1.png.pagespeed.ce.A4LXWNL4hg.png.

8 *О.Турчинов: Національний координаційний центр кібербезпеки повинен мобілізувати весь наявний потенціал для забезпечення надійного кіберзахисту країни - Рада національної безпеки і оборони України*. (б. д.). Рада національної безпеки і оборони України. https://www.rnbo.gov.ua/ua/Diialnist/2528.html?PRINT

9 *Комітет з питань цифрової трансформації інформує як посилити кіберзахист підприємствам та установам.* Офіційний портал Верховної Ради України. https://www.rada.gov.ua/news/razom/221800.html.

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

Irina R. Maltseva
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-6073-4637
irenagold2402@gmail.com

Yuliya O. Chernish
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-6626-5656
kobernikoi@ukr.net

Roman M. Shtonda
Head of Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-5986-0847
shtonda1982@ukr.net

ANALYSIS OF SOME CYBER THREATS IN WAR

Abstract. This article examines the most famous and high-profile cyber threats that were carried out against the state during the Russian invasion. We also analyzed the laws that were adopted during the hostilities on the territory of our state. They have significantly affected the protection against further threats to the entire system.

The issue of Russia's destructive and destructive cyberattacks before the invasion of our country proves that cyberattacks play an important and strategic role in today's world and war, regardless of whether the public is aware of it. This threat is constant for us and it does not stand still and develops. Cyberattacks pose significant problems to our system and infrastructure with paradoxical consequences.

Ukraine's security depends significantly on cybersecurity. This should not only focus attention, but even make every effort. Technological progress will grow, and behind it the dependence in cyberspace. It should be noted that the legislative regulation of relations also has its needs for constant updating and support of the rapid development of technological processes.

Key words: cyber attacks, cyber threats, cyber defense, cyberspace

REFERENCES

1 Veselova, L. Yu. (2021). Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoi viiny [Dys. d-ra]. http://oduvs.edu.ua/wp-content/uploads/2016/06/Disertatsiya_Veselovoi_L.YU..pdf.

2 Shcho take fishynh i yak vid noho zakhystytysia? https://www.tecnoseguro.com/media/k2/items/cache/a7ac92c0202d08b485ecb09c07ac6372_XL.jpg.

3 Bezpeka u kiberprostori. Holovna. https://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1126-bezpeka-u-kiberprostori.

4 https://jurliga.ligazakon.net/. (2022, 13 kvitnia). Borotba z kiberzlochynnistiu v umovakh dii voiennoho stanu: Zakon 2149-IX | YuRLIHA. YuRLIHA. https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix

5 Viina rosii proty ukrainy pochalasia z kibernapadu na suputnyky. za hodynu do vtorhnennia buly znyshcheni «desiatky tysiach» terminaliv Viasat - itc.ua. ITC.ua. https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/

6 Kanada nadaie ukraini rozviddani pro kiberzahrozy – tokar.ua. Tokar.ua. https://tokar.ua/read/48906

7 Iak malomu biznesu zakhystyty sebe vid kiberzahroz. https://businessviews.com.ua/files/news_tape/images/20/40/picture_jak-malomu-biznesu-z_2040_s1.png.pagespeed.ce.A4LXWNL4hg.png.

8 O.Turchynov: Natsionalnyi koordynatsiinyi tsentr kiberbezpeky povynen mobilizuvaty ves naiavnyi potentsial dlia zabezpechennia nadiinoho kiberzakhystu krainy - Rada natsionalnoi bezpeky i oborony Ukrainy. (b. d.). Rada natsionalnoi bezpeky i oborony Ukrainy. https://www.rnbo.gov.ua/ua/Diialnist/2528.html?PRINT

9 Komitet z pytan tsyfrovoi transformatsii informuie yak posylyty kiberzakhyst pidpryiemstvam ta ustanovam. Ofitsiinyi portal Verkhovnoi Rady Ukrainy. https://www.rada.gov.ua/news/razom/221800.html.