DOI https://doi.org/10.30525/978-9934-26-223-4-132

РОСІЙСЬКО-УКРАЇНСЬКА ВІЙНА (2014–2022): КРИЗОВЕ РЕАГУВАННЯ У СФЕРІ ОБОРОНИ; ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЕРЖАВИ

Устименко О. В.

Постановка проблеми. 20 лютого 2014 року розпочалась збройна окупація Криму. Саме цю дату Верховна Рада визнала офіційно початком тимчасової окупації Кримського півострова. 24 лютого 2022 року, тобто через 8 років, почався новий етап війни. Україна стійко, 60-й день (***тобто 2 місяці***), протистоїть російському вторгненню. За час війни агресор зазнав масштабних втрат, так і не досягнувши бажаних результатів, продовжує ракетні атаки та нарощує сили на сході країни. Завдяки успішним діям ЗС України, мирне життя повертається до Києва та десятків інших міст. Але разом з тим відкривається страшна правда про звірства ворога проти мирних жителів на територіях, які були в окупації.

До початку повномасштабного вторгнення Росії в Україну президент держави-терориста Володимир Путін оголосив, що планує провести «спеціальну воєнну операцію», однією з так званих причин якої була «демілітаризація».

Президент України Володимир Зеленський стверджує, що Україні потрібне важке озброєння, щоб захистити життя своїх громадян і протистояти російській армії, яка має кількісну перевагу в особовому складі й техніці. Про це Глава держави наголошує на переговорах з усіма іноземними партнерами. Пріоритетним для нього є питання надання Україні важкого озброєння.

Водночас станом на 23 квітня 2022 року українські військові «отримали» від РФ більше техніки (танки, бойові броньовані машини, тощо), ніж від будь-якої з країн-партнерів, але її теж необхідно ремонтувати.

Аналіз останніх досліджень і публікацій свідчить, що під час анексії Криму у 2014 році, та після цього, Росія провела низку кібератак, щоби дестабілізувати економічну ситуацію в Україні, порушити захист об'єктів критичної інфраструктури, охорони державної таємниці та службової інформації, забезпечення кібербезпеки.

Виклад основного матеріалу. Стратегія забезпечення державної безпеки є основою для розроблення відповідних програмних документів у сфері забезпечення державної безпеки та нормативно-правових актів щодо розвитку складових сил безпеки України, зокрема з питань: контррозвідувальної діяльності; удосконалення механізмів та інституційної спроможності суб'єктів боротьби з тероризмом, транснаціональною та організованою злочинною діяльністю, що використовується іноземними спецслужбами, терористичними організаціями та незаконними збройними формуваннями; захисту об'єктів критичної інфраструктури; охорони державної таємниці та службової інформації; забезпечення кібербезпеки.

Реалізація положень Стратегії наддасть змогу: створити ефективну систему забезпечення безпеки державної таємниці та службової інформації, здатну протистояти викликам сьогодення та забезпечити інтеграцію сектору безпеки і оборони в безпековий євроатлантичний простір[1].

Вищі ступені бойової готовності.

Під час анексії Російською Федерацією Криму та міста Севастополь, у 2014 році, механізми приведення у вищі ступені бойової готовності частин і підрозділів ЗС України виявилися неефективними оскільки система стратегічного керівництва обороною не була готова до цього. В Законі України «Про національну безпеку України»[2] «визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони».

Чи можливо інтегрувати ситуаційні центри профільних органів державної влади сектору безпеки і оборони, як резервний контур управління, в систему стратегічного керівництва обороною, а саме в систему приведення у вищі ступені бойової готовності підрозділів і частин сил оборони?

---

[1] Про Стратегію забезпечення державної безпеки : Указ Президента України № 56/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року. URL: https://www.president.gov.ua/documents/562022-41377 (дата звернення: 07.04.2022).

[2] Про національну безпеку України : Закон України затв. Указом Президента України від 21 черв. 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 07.04.2022).

Це доцільно зробити з метою підвищення її спроможностей реагувати на виклики й загрози національній безпеці України[3].

Шляхи вирішення окремих проблемних питань, щодо удосконалення механізмів приведення у вищі ступені бойової готовності підрозділів і частин складових сил оборони автором висвітлено на міжнародній науково-практичній конференції «Стан та перспективи реформування сектору безпеки і оборони України»[4], а мережу ситуаційних центрів сектору безпеки і оборони, як єдиний організаційно-технічний комплекс, в умовах кризового реагування у сфері оборони, розглянуто у ході IX Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави»[5] тощо. У процесі створення системи ситуаційних центрів складових сектору безпеки і оборони доцільно передбачити можливість їх використання як резервної системи приведення у вищі ступені бойової готовності частин і підрозділів сил оборони.

Метою цієї роботи є розробка моделі резервної системи приведення у вищі ступені бойової готовності підрозділів і частин сил оборони України. Зазначену систему пропонується створити на базі ситуаційних центрів державних органів, що входять до сектору безпеки і оборони. Ефективне управління у сфері оборони повинно передбачати відповідні механізми приведення у вищі ступені бойової готовності підрозділів і частин складових сил оборони України.

Ситуаційний центр це організаційно-технічна система, яка забезпечує збір, накопичення, обробку і аналіз інформації (моніторинг), необхідної для прогнозування, планування та прийняття рішень у сфері національної безпеки і оборони[6]. Передбачалося, що органи державної влади будуть подавати результати моніторингу до Апарату Ради національної безпеки і оборони України через Головний ситуаційний центр України щоквартально. У разі необхідності, на вимогу Секретаря Ради національної безпеки і оборони України окремі органи державної влади результати моніторингу надаватимуть частіше. Водночас, у разі виявлення під час моніторингу раптових змін індикаторів, які свідчать про різке погіршення стану національної безпеки України, орган державної влади зобов'язаний невідкладно надати результати моніторингу до Апарату Ради національної безпеки і оборони України[7].

На нашу думку доцільно передбачити можливість, щоб у разі низького (критичного) рівня національної безпеки України відповідні сигнали з ситуаційних центрів надходили не лише на Головний ситуаційний центр України, а звідти через Апарат РНБО України до керівництва держави, а й до частин і підрозділів сил оборони, активізуючи механізми приведення у вищі ступені бойової готовності. Модель зазначеної системи приведення у вищі ступені бойової готовності підрозділів і частин сил оборони зображена на рис. 1[8].

Якщо за результатами моніторингу на Головному ситуаційному центрі України буде визначено, що чисельне значення відповідного індикатору свідчить про досягнення критичного рівня національної безпеки України, то відповідні сигнали з відомчих ситуаційних центрів будуть оперативно надходити не лише до Апарату Ради національної безпеки і оборони України та керівництва держави, а й до частин і підрозділів сил оборони, активізуючи механізми приведення у вищі ступені бойової готовності.

Однак ситуаційні центри нині є лише аналітичними структурами і необхідно внести зміни в чинне законодавство, щоб ситуаційні центри набули спроможностей органів військового управління, при виникненні кризових ситуацій, що загрожують національній безпеці України.

Але нині більше уваги приділяється силам територіальної оборони. В цьому і є проблема. Адже потрібно виділення відповідних коштів і ресурсів для їх формування чи доукомплектування. Президент України Володимир Зеленський доручив головам ОДА їх доукомплектувати – «Я хотів би звернутися до голів обласних державних адміністрацій, а також до голови Київської міської державної адміністрації для того, щоб ви за два тижні все зробили, без імпровізацій. Консультуйтеся з нашими військовими згідно із законодавством про Національний спротив. Ми не маємо часу щось шукати, вирішувати, займатися політикою».

---

[3] Оборонний менеджмент: управління процесами: монографія / Саганюк Ф. В., Устименко О. В., Мудрак Ю. М., Павленко В. І. Київ : Видавничий дім «АртЕк», 2021. 324 с.

[4] Устименко О. В. Удосконалення механізмів приведення у вищі ступені бойової готовності підрозділів і частин складових сил оборони. *Стан та перспективи реформування сектору безпеки і оборони України:* матеріали міжнародної науково-практичної конференції 24 лист. 2017 р.: у 2 т. Київ.: Національна академія прокуратури України, Т. 1. С. 425–427.

[5] Устименко О. В. Мережа ситуаційних центрів сектору безпеки і оборони як єдиний організаційно-технічний комплекс в умовах кризового реагування у сфері оборони. *Актуальні проблеми управління інформаційною безпекою держави:* зб. тез наук. доп. наук.-практ. конф., Київ, 30 березня 2018 р.: Нац. акад. СБУ, 2018. С. 174 –179.

[6] Устименко О. В. Моніторинг національної безпеки як складова механізму стратегічного планування. *Вісник НАДУ*. 2016. № 4. С. 50–55.

[7] Устименко О. В., Пеньковський В.І. Індикатори (показники) стану за проміжок часу. *Науково-інформ. вісник Академії національної безпеки*. 2016. № 1-2 (9-10). С. 62–75.

[8] Устименко О. В. Розробка моделі системи приведення у вищі ступені бойової готовності підрозділів і частин сил оборони на базі ситуаційних центрів державних органів. *Державне будівництво.* Електронне наукове фахове видання Національної академії державного управління при ПУ України.

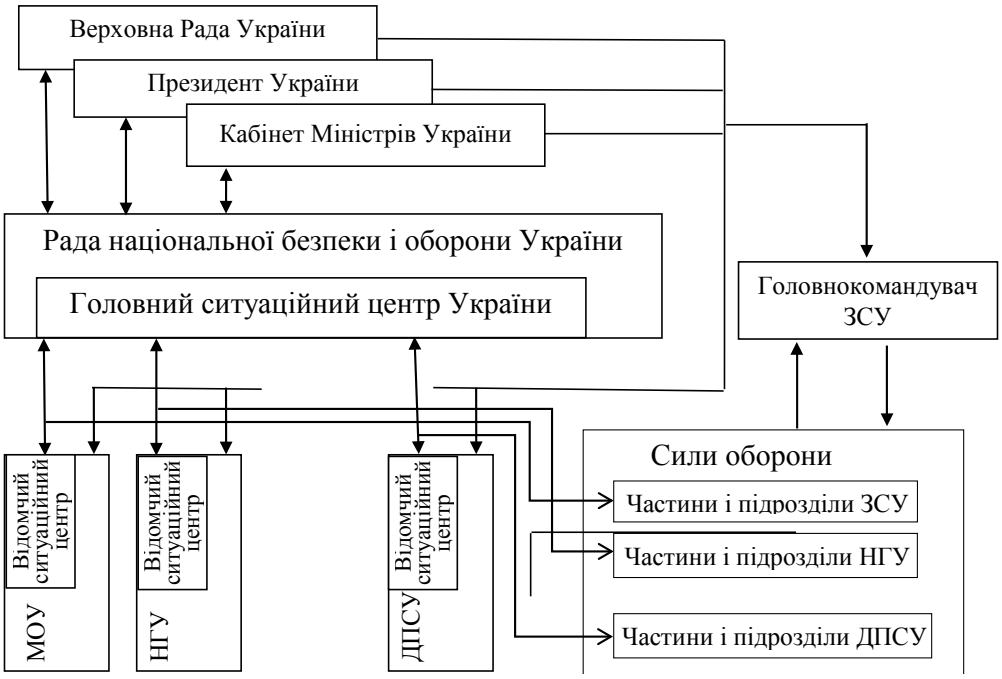


Рис. 1. Модель резервної системи приведення у вищі ступені бойової готовності підрозділів і частин сил оборони

Приведення столиці України у вищі ступені бойової готовності.

Розглянемо як функціонує система забезпечення столиці. Згідно інформації, що поступає через засоби масової інформації, об'єкти критичної та соціальної інфраструктури Києва працюють в режимі підготовки до роботи в умовах надзвичайної ситуації. Київ має розгалужену та складну інфраструктуру життєзабезпечення, стабільна робота якої в надзвичайній ситуації – чи не найголовніше завдання.

Зусилля столичної влади спрямовані на те, щоб упередити чи подолати як можливі провокації, так і вистояти в умовах військового нападу. Саме про це мер Києва Віталій Кличко повідомив у п'ятницю, 11 лютого 2022 року[9].

«Створені запаси палива, встановлені електрогенератори для безперебійної роботи в надзвичайній ситуації систем управління містом та ТЕЦ столиці на період до 10 діб. Підприємства забезпечені гарантованим безперебійним зв'язком на випадок відсутності мобільного зв'язку та інтернету», – написав Кличко. Він повідомив, що вдосконалює столицю і систему оповіщення, аналогів якої в Україні немає. На її будівництво планується виділити з бюджету міста близько 11 млн грн.

«За кілька останніх років збільшили кількість укриттів утричі. Загалом до фонду захисних споруд цивільного захисту входять понад 500 сховищ та майже 4500 споруд подвійного використання (підземних паркінгів і переходів, заглиблених станцій метро, підвалів та напівпідвалів). У Києві створені комісії з питань евакуації – на рівні КМДА та в кожному районі. Затверджений План евакуації населення. Він визначає місця розташування збірних евакуаційних пунктів, кількість необхідного транспорту та безпечні райони для розміщення населення», – наголосив Кличко.

Мер Києва Віталій Кличко разом зі своїм братом Володимиром закликали киян вступати до територіальної оборони (ТРО). Міський голова столиці опублікував відео з навчань повного складу 112 бригади територіальної оборони, участь у яких одночасно взяли 9 батальйонів[10].

5 лютого, у суботу, кияни тренувалися, складали присягу, приймали до своїх лав новобранців. Одноденні навчання під час зборів проходили на десятьох майданчиках, де учасники вивчали основи орієнтування на місцевості, принципи роботи радіообладнання та шифрування повідомлень, відпрацьовували індивідуальні бойові навички, тактику та медичну допомогу в умовах ведення бою. А також навчалися основних принципів поводження з вибуховими пристроями. Крім постійного складу батальйонів тероборони та резервістів, збори відвідали близько 80 новачків-рекрутів, серед яких було багато жінок. За словами інструкторів, за підсумками занять чимало рекрутів висловили бажання укласти контракт резервіста територіальної оборони.

[9] У Києві затвердили план дій на випадок надзвичайної ситуації, – Кличко. URL: https://aspi.com.ua/news/kiiv/u-kievi-zatverdili-plan-diy-na-vipadok-nadzvichaynoi-situacii-klichko#gsc. tab=0 (дата звернення: 13.02.2022).

[10] «Захистимо Україну разом»: брати Клички закликали громадян вступати до тероборони. URL: https://aspi.com.ua/news/kiiv/zakhistimo-ukrainu-razom-brati-klichki-zaklikali-gromadyan-vstupati -do-teroboroni#gsc.tab=0 (дата звернення: 13.02.2022).

Кожен, хто хоче стати на оборону держави, може обрати напрямок служби – приєднатися до резерву Збройних сил України або стати на службу органів територіальної оборони свого регіону. Нагадаємо, загалом ТРО у складі 25 бригад об'єднуватиме понад 150 батальйонів. У кожному з них буде до 600 осіб. Загалом до сил територіальної оборони буде залучено 130 тисяч осіб[11].

Хоча виникає резонне запитання – наскільки будуть боєздатними зазначені підрозділи, які проводять «**одноденні навчання під час зборів**»?

В принципі Українська армія є набагато сильнішою і краще підготовленою, ніж у 2014. Про це йдеться у спільній заяві Міністра оборони та Головнокомандувача Збройних сил України. За словами Міністра оборони нині Україна має найпотужнішу армію за останні 15 років.

«Іловайськ, Дебальцеве залишили шрами на її серці, але загартували волю. Героїчна оборона Донецького і Луганського аеропортів, щоденний захист десятків населених пунктів – від Станиці Луганської до Широкиного – зробили бойовий дух незламним, – каже міністр і запевняє – кожен, хто бодай один раз дивився в очі нашим воїнам, впевнений – повторення 2014 не буде, агресору не взяти ані Київ, ані Одесу, ані Харків, ані будь-яке інше місто».

«420 тисяч українських воїнів і кожен без винятку командир уже дивилися в очі смерті. Ми не віддамо ні клаптика Української землі!», – заявив Головнокомандувач ЗС України генерал-лейтенант Валерій Залужний.

Він також повідомив, що українські вояки постійно вдосконалюють «свої оборонні спроможності, злагодженість підрозділів та військову майстерність», – наприклад, як зараз під час навчань «Заметіль-2022». Крім того, за словами Валерія Залужного, вже створені «бойові порядки і встигли у стислі терміни розгорнути Сили територіальної оборони та озброїли їх ПТРК і ПЗРК».

А Міністр оборони нагадує не лише про дипломатичну, але й про військову підтримку від західних партнерів України: «Протягом місяця від різних країн отримано майже 2000 тон сучасного озброєння, боєприпасів і засобів бронезахисту. Наші воїни вже пройшли навчання і готові застосовувати весь арсенал засобів». Він вважає, що багато країн лише зараз по-справжньому усвідомили небезпеку дій Росії, і тому емоційно реагують на те, через що Україна пройшла вже 8 років тому[12].

І, хоча дії Кремля не може передбачити ніхто, але в Україні розглядають і готуються до багатьох варіантів розвитку подій. «Саме спокій зараз – головна зброя, яка може забезпечити нам надійний фундамент для оборони. Продовжувати звичайне життя, працювати, забезпечувати нормальну економічну діяльність, а отже і можливість Збройних Сил захищати країну так і стільки, як і скільки потрібно» – каже Олексій Резніков.

На півдні України ситуація більш тривожна. Росія передислокує в Чорне море великі десантні кораблі з Балтійського та Північного флотів. На борту цих кораблів, за даними аналітиків Міноборони України, може бути близько тисячі морських піхотинців та 100 одиниць бронетехніки. Іншими словами, повноцінна батальйонно-тактична група, яка здатна десантуватися в прибережній зоні та захопити плацдарм – для подальшого вторгнення.

Кораблі Чорноморського флоту спроможні дістати своїми ракетами цілі в Одесі, навіть не виходячи з Севастополя.

Але врешті далі йти доведеться суходолом, і те, що легкої екскурсії не вийде, в Кремлі добре усвідомлюють. Тому МЗС Росії оголошує свій черговий ультиматум. Вимагає, аби українці віддали назад тисячі тон оборонного озброєння, яке отримали за останній місяць від союзників[13].

Перед нами стоїть завдання щодо захисту інформаційної системи держави.

Формулювання відповідних цілей. Кібервійна між Росією та Україною.

Взаємні кібератаки між Україною та Росією останніми роками стали буденністю. За даними **Служби безпеки України** (СБУ), хакерські угруповання, які підтримує Росія, атакують Україну, називаються **Fancy Bear, Turla** і **The Dukes**. Вони стояли за руйнівними кібератаками в Україні, включаючи **BlackEnergy, Industroyer** та **NotPetya**[14]**.**

Чергова провокація з боку Росії.

Посольство України в Японії прокоментувало написи, які з'явилися на урядових сайтах. На їхню думку, повідомлення має намір ввести в оману. «Робиться вигляд, що це йде з Польщі. Насправді немає жодного сумніву, що це чергова провокація з боку Росії», – йдеться у повідомленні посольства у фейсбуці. «Якщо ви побачите подібне, або інші провокаційні повідомлення й на інших урядових ресурсах – майте на увазі, що **проти України ведеться війна**», – додали у **посольстві**.

[11] Устименко О.В. Приведення сил оборони та столиці України – міста Київ, у вищі ступені бойової готовності Scientific Collection «InterConf», (100): with the Proceedings of the 6th International Scientific and Practical Conference «Global and Regional Aspects of Sustainable Development». Copenhagen, Denmark. Busse Verlag GmbH, February 26-28. 2022. 974 p. С. 965–972.

[12] Росії не взяти Київ, Харків чи Одесу – заява командування ЗСУ. URL: https://www.bbc.com/ukrainian/news-60362776 (дата звернення: 13.02.2022).

[13] На порозі можливої війни: що відбувається на кордонах, у морі та на дипломатичних переговорах. URL: https://tsn.ua/exclusive/na-porozi-mozhlivoyi-viyni-scho-vidbuvayetsya-na-kordonah-u-mori-ta-na-diplomatichnih-peregovorah-1976206.html (дата звернення: 13.02.2022).

[14] СБУ розкрила імена російських хакерів, які атакують Україну з 2014 року. URL: https://enovosty.com/uk/markets-ukr/full/611-sbu-rozkrila-imena-rosijskix-xakeriv-yaki-atakuyut-ukrainu-z-2014-roku (дата звернення: 13.02.2022)..

Речник «**Українського кіберальянсу**», ІТ-експерт Андрій Баранович (відомий як ***Шон Таунсенд***), вказує, що повідомлення про злам сайтів з'явилося у російських ЗМІ через дві години після самого інциденту. «В EXIF картинки координати вказують на парковку біля школи економіки у Варшаві, але я вважаю, що все це зроблено спеціально, щоби розсварити Україну та Польщу», – написав він у фейсбук.

Джо Тайді, **кореспондент BBC** з питань кібербезпеки. Тижнями світ нервово чекав, коли накопичені російські війська перетнуть через кордон з Україною. Аналогічно спільнота кібербезпеки спостерігала й чекала на якесь кібервторгнення. «Гібридна війна» – атаки як у кіберсфері, так і фізичному світі, є частиною сучасного конфлікту. Свою майстерність у цьому Росія довела ще раніше.

Під час вторгнення в Грузію 2008 року урядові вебсайти вимкнули через атаки з боку Росії.

Під час анексії Криму Росією у 2014 році її знову ж таки звинуватили у запуску низки кібератак, щоби дестабілізувати комунікації та поширити плутанину, поки війська захоплювали регіон. Замість кібернаступу, замовленого Кремлем, це більше схоже на скоординовану атаку патріотично налаштованих російських хакерів. Можливо це не є замовленням Кремля, але вони, безумовно, не відмовляться від будь-яких зусиль, щоб ще більше похитнути Україну в цей надзвичайно напружений для країни час.

Атаки на енергокомпанії. Одна з останніх масштабних хакерських атак відбулася в 2017 року. 27 червня 2017 року вірус «**Petya.A**» паралізував мережі багатьох українських компаній та органів влади. В Україні вірус заразив комп'ютери кількох міністерств, енергетичних компаній, банків, ЗМІ, мобільних операторів, мереж заправок, київського аеропорту Бориспіль і київського метро.

Не працював також і офіційний сайт Кабінету міністрів України, але згодом його роботу відновили.

СБУ заявила про причетність російських спецслужб до цієї атаки. Посилаючись на дані, СБУ вказувала на ті ж самі хакерські угрупування, які у **грудні 2016 року атакували фінансову систему, об'єкти транспорту та енергетики** України.

У 2015 році кілька українських обласних енергорозподільчих компаній стали жертвами кібератаки, яка призвела до відімкнення світла у десятків тисяч споживачів. Найбільш масштабним за наслідками виявився напад на «**Прикарпаттяобленерго**». Тоді впродовж кількох годин були знеструмлені десять районів Івано-Франківської області.

Тоді ж Державна служба спецзв'язку і захисту інформації повідомила про спробу «інфікувати» комп'ютери міжнародного аеропорту «Бориспіль» тим самим вірусом, що використовувався при нападах на енергокомпанії.

У грудні 2016 року кібернападу зазнали державне казначейство, міністерство фінансів та пенсійний фонд. Через них на кілька днів були заблоковані бюджетні платежі на сотні мільйонів гривень, а сайти мінфіну і казначейства не працювали[15].

Викладення основного матеріалу. Система кібербезпеки України має багато проблем і вразлива до кремлівських атак, але українська влада хоче приховати ці факти від суспільства, пише ***The Times***. Про це виданню розповів ***Шон Таунсенд***, якого видання називає провідним хакером України. «***Влада боїться того, наскільки незахищеними є наші інформаційні системи, але хоче приховати це від суспільства***», – цитує Барановича газета.

Масштаб та інтенсивність кібератак проти України стурбували НАТО та уряди Заходу, які бояться, що такі операції будуть здійснені проти них.

Лише на початку липня Державна служба спецзв'язку та захисту інформації повідомляла про кібератаки на сайти Президента України та спецслужб. Імовірно, за цим стояла Росія, пише ***The Times***. Видання також пригадує інші атаки на Україну, за якими могла стояти Росія. Зокрема, напад на виборчу комісію в 2014 році, атаку на *українські банки в 2017 році* та удар по *українській енергетичній мережі* через шкідливе програмне забезпечення **Black Energy**, від якого постраждали понад 230 тис. людей.

Щоправда, Москва послідовно заперечує свою причетність до будь-яких кібератак за кордоном.

Газета ***Times*** нагадує, що ***Шон Таунсенд*** (Sean Townsend) став відомим у 2014-му, коли створив ***хакерську групу RUH8***. «У нашої країни **в 2014-му році взагалі не було знань у галузі кібербезпеки,** – розповідає активіст. – Україну атакували військові та хакери, тому я вирішив допомогти нашій країні боротися з росіянами, здійснюючи проти них хакерські атаки у відповідь». RUH8 став частиною колективу «хактивістів», які зламували інформаційні системи російських військових частин, розвідки, регіональних урядів та верхньої палати російського парламенту.

Згодом ці групи об'єдналися в громадську організацію «Український кіберальянс», яка злила електронні листи, що ймовірно належали Владиславу Суркову – екс помічнику президента РФ Володимиру Путіну, якого називали неформальним куратором українського питання в Кремлі.

Ці листи містили детальні плани з анексії Криму та підбурювання до сепаратизму на Донбасі.

У 2018-му RUH8 почав тестувати інформаційну безпеку українського уряду. «Не використовуючи спеціальні пристрої, ми отримали доступ до комп'ютерів міністерств юстиції та охорони

[15] Хакери атакували урядові сайти. Сайт «Дії» також не працював. Хто стоїть за кібератакою? URL: https://www.bbc.com/ukrainian/news-59991859 (дата звернення: 13.02.2022).

здоров'я. Ми виявили, що навіть атомні електростанції є вразливими», – каже хакер. Влада хвалила Барановича за хакерські операції поти Росії, однак зріклася його після того, як той ***виявив прогалини в здатності України захищати себе***, пише газета.

У лютому 2020 року в засновників «Українського кіберальянсу» провели обшуки. Активісти розцінили це як тиск і припинили співпрацю з державними та правоохоронними структурами України.

Баранович наполягає, що відносини між «Українським кіберальянсом» та спецслужбами були неформальними. «Якщо ми знаходили щось дуже цікаве, ми передавали це нашим спецслужбам, яким довіряли. Але не було офіційних відносин», – каже він. Хакер додав, що кібершпигунство є надзвичайно ефективним. «Це майже нічого не коштує. Якщо вам потрібно було щось дізнатися під час Холодної війни, держава мала інвестувати величезні гроші, тренування, досвід, час… Тепер ви можете знайти кібернайманця, який зламає систему електронної пошти за сто баксів», – пояснює він[16].

14 січня 2022 року Кібернападу зазнали 70 сайтів центральних та місцевих органи виконавчої влади.

Про це розповів на брифінгу заступник голови Держспецзв'язку з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктор Жора, передає Укрінформ. «З 13 на 14 січня цього року було здійснено хакерську атаку на сайти державних органів України. На їх головних сторінках були розміщені повідомлення провокаційного характеру. Можу відразу наголосити, що персональні дані українців жодним чином не спотворені, витоку даних не відбулось, а контент сайтів не ушкоджений», – розповів Віктор Жора.

За його словами, ця кібератака є одною з найпотужніших за останні кілька років – зазнало ураження близько 70 сайтів центральних та місцевих органи виконавчої влади. Частина з них працювала, інша – була призупинена з метою недопущення поширення атаки на інші державні ресурси та локалізації технічної проблеми.

Заступник керівника Держспецзв'язку наголосив, що поки достеменно невідомо, хто причетний до кібератаки на урядові сайти. «Тут слід розуміти, що говорити про причетність тієї чи іншої сторони до кібератак можна лише **після повномасштабного розслідування інциденту**. Як тільки будуть безперечні цифрові докази та розуміння того, що сталось, ми зробимо відповідну заяву», – підкреслив Віктор Жора.

Держспецзв'язку спільно зі СБУ, Кіберполіцією та міжнародними партнерами займалися розслідуванням інциденту та розбирали цифрові докази[17]. Крім того необхідно зазначити, що в січні 2022 року планувалося, що в Україні з'являться **кібервійська**. В Міністерстві оборони України модернізувалися територіальні центри комплектування та соціальної підтримки.

Міністр оборони Олександр Рєзніков розповів як він бачить цей процес і яким чином будуть працювати колишні військкомати. Передбачалося, що будуть введені цифрові технології як для організації управлінських процесів, так і для розробки воєнної тактики ведення бою.

Найближчим часом планувалося ввести автоматизовані системи управління військами різних рівнів. Серед нововведень – створення «Воєнних ЦНАПів» (Центр надання адміністративних послуг) чи рекрутингових центрів для набору військових на службу по контракту в Збройних Силах чи Силах територіальної оборони. В зв'язку з цим був розроблений проект модернізації територіальних центрів комплектування по принципу дії ЦНАП, в зв'язку з чим проходив погодження пакет відповідних документів для її реалізації.

Планувалося що в Україні з'являться **кібервійська** для захисту від зовнішніх загроз. До їх лав будуть відбирати кращих фахівців, щоб вони працювали на благо країни і посилили безпеку державних реєстрів та ресурсів. Після реформ українська армія повинна була стати більш професійною, а Міністерство оборони – одним із кращих роботодавців[18].

Втім у ніч проти 14 січня 2022 року хакери масово атакували українські урядові сайти. Йдеться про сайт уряду, окремих міністерств і навіть сайт застосунку «Дія». У СБУ кажуть, що витоку персональних даних не було.

В ЄС засудили атаку на українські урядові сайти та заявили про готовність допомогти. З самого ранку п'ятниці не працювали сайти Кабінету міністрів, МЗС, ДСНС, МОН, мінспорту, міненерго, мінагрополітики, міністерства у справах ветеранів та сайт держказначейства.

На сайті міністерства закордонних справ та деяких інших можна було побачити таке повідомлення: «Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі» (рис. 2.).

[16] Влада приховує вразливість кіберсистеми України – хакер в інтерв'ю Times. URL: https://www.bbc.com/ukrainian/news-57886765 (дата звернення: 13.02.2022).

[17] Кібератаки зазнали 70 сайтів органів влади, – Держспецзв'язку. URL: https://biz.censor.net/news/3310090/kiberataky_zaznaly_70_sayitiv_organiv_vlady_derjspetszvyazku (дата звернення: 13.02.2022).

[18] Аналоги ЦНАПов и кибервойска: как модернизируют армию и бывшие военкоматы. URL: https://protect.comments.ua/news/2022/analogi-cnapov-i-kibervoyska-kak-moderniziruyut-armiyu-i-byvshie-voenkomaty-693234.html (дата звернення: 13.02.2022).

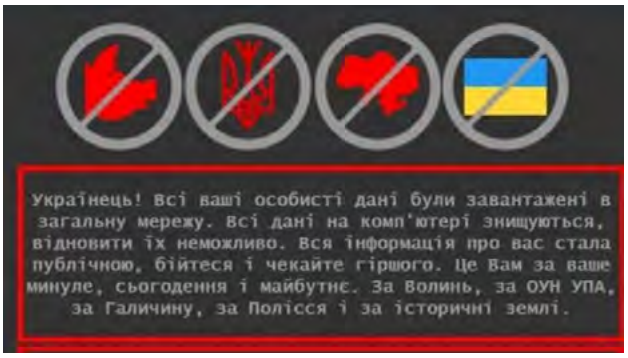


Рис. 2. Повідомлення на сайті

Повідомлення було опубліковане українською, російською та польською мовами. Пізніше його прибрали, а самі сайти просто перестали відкриватися.

Жозеп Боррель, верховний представник ЄС з закордонних справ, засудив атаки на українські сайти та заявив, що Євросоюз готовий допомогти Україні захиститися. «Ми плануємо мобілізувати всі наші ресурси, щоб допомогти Україні впоратися з цією атакою. На жаль, ми знали, що це може статися», – заявив він на зустрічі міністрів закордонних справ країн ЄС у французькому Бресті.

А **глава МЗС Швеції Анн Лінде** підтримала Україну і закликала до жорсткої позиції щодо Росії. «Якщо відбуватимуться атаки проти України, ми будемо дуже суворими та рішучими у нашій відповіді», – додала вона перед зустріччю міністрів ЄС, пише «Інтерфакс-Україна».

«Ми стурбовані інформацією про кібератаку на сайти українського уряду, в тому числі на сайт МЗС. Ми рішуче засуджуємо будь-яку діяльність, яка має наслідком поширення дезінформації та порушення функціонування державних інституцій», – написав у Twitter **речник МЗС Польщі Лукаш Ясіна**.

СБУ, кіберполіція та держспецзв'язку розслідують інцидент та збирають цифрові докази. Більшу частину постраждалих державних ресурсів вже відновили, додали в СБУ.

У відомстві закликали користуватися іншими вебресурсами, зокрема офіційними сторінками міністерств у соцмережах.

Раніше в інтерв'ю **BBC News Україна** міністр цифрової трансформації Михайло Федоров, відповідальний за розробку і впровадження «Дії», запевняв, що всі персональні дані українців надійно захищені. У Мінцифри запевнили, що «**Дія**» – безпечний продукт, а портал зараз відключили, як і низку інших урядових сайтів, щоби не допустити поширення атаки на інші ресурси. Якщо спробувати зайти на сайт «**Дії**» зараз, то користувача автоматично переадресовують на сайт *www.plan2.diia.gov.ua*, який працює у штатному режимі. Але точки входу на портал для завантаження документів там немає.

За даними **Cisco**, компанія **Armagedon** вже давно пов'язана із проросійською діяльністю. За даними Cisco, більшість IP-адрес пристроїв хакерів також ведуть до Росії. Навіть назва групи – Armagedon – використовує російське написання слова «Армагеддон» з одним «д».

На записах, отриманих СБУ, кіберзлочинці обговорювали свої зарплати та відсутність винагороди з боку керівництва ФСБ Криму. Хоча хакерів не було затримано, розслідування СБУ може змусити Росію захистити їх.

За словами прес-секретаря **Українського кібернетичного альянсу**, який працює під ім'ям **Шон Таунсенд**, Україні також слід очікувати атаки у відповідь. «Ми маємо чекати її від ФСБ, тому що вона дуже чутлива до українських новин», – написав він у Facebook.

В Україні кібератаки зазнали деякі урядові сайти. Зокрема портали **Верховної Ради, Кабінету Міністрів, Служби безпеки України** та **Міністерства закордонних справ** не відкриваються.

Доступ до урядових сайтів відсутній. При спробі зайти на один із них видається помилка. Також із труднощами працюють сайти **Міністерства оборони** та **Міністерства внутрішніх справ.**

Спікер Верховної Ради заявив, що хакери спробували зламати акаунти його сім'ї та заблокувати банківські картки. Зазначимо – спроби входу здійснювалися з Росії.

Зазначимо, що кібератаку здійснили і 15 лютого. Вона стала наймасштабнішою в історії. **DDoS**-атаки, тобто перевантаження трафіку сайтів, тривали й 16 лютого. Тоді хакери знайшли вразливі місця у програмному коді самого сайту. Для ліквідації наслідків залучали українських та американських фахівців.

Зокрема кібер-напад, який здійснили вночі 14 січня був ініційований РФ. Майже всі державні інформаційні ресурси 17 січня відновили роботу.

Скільки кібератак на державні органи України зупинили фахівці у 2021 році – на інфографіці (рис. 3). Ситуація на 15 лютого 2022 року.

«Вчора, 15 лютого, було здійснено наймасштабнішу в історії України **DDoS**-атаку на урядові сайти, банківський сектор. Вчора всі органи, які відповідають за кібербезпеку, працювали, щоб протистояти цим атакам та ліквідувати їх найближчим часом», – сказав він. За його словами, ця атака готувалася наперед, її вартість становить мільйони доларів. Метою було дестабілізувати ситуацію та посіяти паніку.

Заступник голови Держспецзв'язку Віктор Жора зазначив, що станом на кінець лютого в Україні **DDoS**-атаки продовжуються. Фахівці вживають усіх заходів. «Наразі ситуація контрольована. Атака продовжується. Середні показники потужності атаки досягають десятків гігабіт на секунду. Ми фіксуємо

Рис. 3. Кібератаки на держоргани України (на 15 лютого 2022 року)

комбінацію методів, тобто цілу низку технологій атаки на ресурси, що свідчить про координацію дій атакуючих, про залучення великого обсягу ресурсів, але ми впораємося», – додав він. За даними Держспецзв'язку, вчорашня **DDoS**-атака та кібератака на держсайти 14-15 січня – відрізняються технологічно, але схожі за масштабом та рівнем підготовки. Нагадаємо, увечері 15 лютого у роботі сервісів державного Приватбанку спостерігалися масштабні збої. Також були атаковані хакерами сайти Міноборони та ЗС України[19].

15 лютого Білий дім заявив, що владі США відомо про кібератаки в Україні проти низки сайтів органів влади та ресурсів державних банків. Як пише ***Reuters***, Вашингтон готовий надати підтримку Києву в розслідуванні та реагуванні на цей інцидент.

Співзасновник **monobank** Олег Гороховський у ***Facebook*** зазначав, **DDoS**-атака була направлена «на майже всі українські банки з різною результативністю». Також вони були направлені на **monobank, «Альфа-банк** та «**А-банк**». Останні атаки були зафіксовані з вузла в Нідерландах.[20]

Раніше Європейський центральний банк попереджав про можливі кібератаки на банки з боку Росії. **Британський національний центр кібербезпеки** також попередив великі організації, щоб зміцнили свою стійкість до кібербезпеки на тлі поглиблення напруги навколо України.[21]

24 лютого 2022 – цинічний напад Росії на Україну, створення української ІТ-Армії.

Створення української ІТ-Армії.

У ніч вторгнення РФ ворог хотів знищити весь кіберзахист України. З початку повномасштабної агресії РФ оперативно виявлено та нейтралізовано більше 120 потужних кібератак на ресурси органів державної влади та військового управління України. Найбільша їх кількість припала на ніч вторгнення – саме тоді ворог хотів знищити весь кіберзахист України. Втім ефективна робота СБУ та інших органів кібербезпеки не дозволила агресору використати кіберпростір для отримання військових переваг.

Військова агресія Росії не обмежилася атаками на цивільне населення та бомбардуванням міст. Кібератаки обрушилися на сайти українських ЗМІ, сервіси та державні сайти. Стало зрозуміло, що потрібно чинити опір і завдавати удару у відповідь. Було прийнято рішення сформувати **ІТ-Армію** з найкращих спеціалістів у галузі і створена була за лічені години.

Долучитися запропонували: **розробникам, кіберспеціалістам**, **дизайнерам, копірайтерам, маркетологам, таргетологам та іншим фахівцям.**

Головними завданнями ІТ-Армії України стали протистояння ворогу у кіберпросторі та поширення достовірної інформації про війну, яку Росія розв'язала в Україні. Від часу створення ІТ-Армії вона добилася вражаючих успіхів на кібер-фронті:

Кібервійська зламали сайт Кремля та виклали

[19] Остання кібератака на банки та держсайти була наймасштабнішою в історії – Мінцифри. URL: https://www.slovoidilo.ua/2022/02/16/novyna/ suspilstvo/nova-kiberataka-banky-ta-derzhsajty-bula-najmasshtabnishoyu-istoriyi-mincyfry (дата звернення: 13.02.2022).

[20] США готові допомогти Україні у розслідуванні кібератаки на ресурси держбанків та органів влади. URL: https://biz.censor.net/news/3316506/ssha_gotovi_dopomogty_ukrayini_u_rozsliduvanni _kiberataky_na_resursy_derjbankiv_ta_organiv_vlady (дата звернення: 18.02.2022).

[21] Сайти Верховної Ради, Кабміну, СБУ та МЗС не працюють через кібератаку. URL: https://bykvu.com/ua/bukvy/saity-verkhovnoi-rady-kabminu-sbu-ta-mzs-ne-pratsiuiut-cherez-kiberataku/ (дата звернення: 25.02.2022).

у мережу номери телефонів усіх працівників, а міністр МВС Вадим Денисенко закликав кожного українця телефонувати на номери.

Головний російський біржевий холдинг – **Московська біржа – впала за 5 хвилин** від початку роботи у понеділок, 28 лютого.

На каналі **IT ARMY of Ukraine** з'явилося повідомлення: «Росіяни конвертують криптовалюту в євро через рублі і назад на цей ресурс. Ви знаєте, що робити».

Через дві хвилини українські кіберназівці «зруйнували» біржу після повідомлення про те, що росіяни використовують цей ресурс для конвертації рублів. Про це з посиланням на **Telegram-канал** кібервиборців – **IT ARMY Of Ukraine** заявив міністр цифрової трансформації Михайло Федоров[22].

*Станом на 28 лютого фінансова система фактично обвалилася в Росії. Зокрема, вранці Центробанк Росії прийняв рішення підвищити ключову ставку з **9%** до **20%** річних, що фактично припиняє кредитування російської економіки.*

Практично відразу після цього війська ІТ-Армії поклали і сайт російського «**Сбербанку**».

Не пройшло й багато часу, як того ж дня завис сайт **ФСБ**.

Разом з тим в соцмережах та на інших ресурсах почали з'являтися інформаційні повідомлення спрямовані на громадян Росії із закликами припинити війну та не відпускати своїх родичів до України.

Українська ІТ-Армія за останній тиждень, з 11 до 17 квітня, атакувала понад 135 онлайн-ресурсів росії.

Так, у результаті атаки на російську національну систему маркування товарів міністерство промисловості рф було змушене дозволити виготовляти та продавати товари без QR-кодів. Згодом воно заявило, що певний час будуть жити без цієї системи. Атака системи рф для стягнення оплати за проїзд вантажними автомобілями, масою від 12 тон, створила значні перепони вантажному транспорту в пересуванні автомагістралями[23].

СБУ попросила українців повідомляти про уразливості в комп'ютерних мережах, електронній пошті або месенджерах окупанта.

«За останні кілька днів ми отримали багато корисної інформації про пересування противника і його розвідувальних груп. Завдяки вам багато окупантів було знищено!

І відсьогодні в чат-боті з'явилася нова функція – боротися на кібер-фронті...[24]

З дня цинічного нападу Росії на Україну війна триває на лише на фронті, але й в інформаційному та цифровому напрямках. За дні протистояння українські кібервоїни досягли неймовірних результатів про які просто неможливо забути.

Активно включилися в боротьбу з агресорами, після нападу Росії, і фахівці і промисловці.

Підтримка групи хакерів Anonymous.

З моменту атаки Росії на Україну свою підтримку українцям висловили, у свій оригінальний спосіб, і хакери відомої в усьому світі децентралізованої групи під назвою **Anonymous**.

Лише протягом 26 лютого кількість **DDoS**-атак на російські урядові сайти перевалила за 50 у понад 1 Терабайт. Хакерам вдалося покласти сайти: ***Кремля, Держдуми, «Першого каналу», «Роскосмосу» і «Російської залізниці».***

Згодом вони навіть записали особисте звернення до Владіміра Путіна, де наголосили, що зовсім скоро світ та громадяни Росії дізнаються жахливу правду, яку від них приховує російський диктатор.Наступного дня **Anonymous** атакували низку російських урядових сайтів серед яких і сайт Кремля. Хакери виклали у вільний доступ поштові адреси та паролі співробітників установи.

Згодом була здійснена атака на російські телеканали. На них з'явилися відео з висвітленням реальної ситуації в Україні та закликом не відправляти російських солдат в Україну. Після цього хакери зламали низку сайтів найбільших ЗМІ Росії та розмістили на інформаційні повідомлення із різними закликами до росіян на підтримку України.

7 березня 2022 року хакери зламали російські стримінгові сервери **Wink** та **Ivi** й онлайн трансляцію телеканалів «Перший», «Росія 24» і «Москва 24». Замість новин цих каналів вони запустили передплатникам кадри бомбардування Харькова. Усе це щоправда, тривало недовго: дуже швидко звичайну трансляцію було відновлено[25].

[22] Українські кіберназівці «зруйнували» біржу, де росіяни намагалися конвертувати рублі у валюту. URL: https://zn.ua/ECONOMICS/ukrainskie-kibervojskie-obvalili-birzhu-hde-rossijane-pytalis-konvertirovat-rubli-v-valjutu.htm (дата звернення: 05.03.2022).

[23] Українська ІТ-армія за тиждень атакувала понад 135 ресурсів росії. URL: https://rubryka.com/2022/04/18/ukrayinska-it-armiya-za-tyzhden-atakuvala-ponad-135-resursiv-rosiyi/ (дата звернення: 18.04.2022).

[24] СБУ попросила помощи на киберфронте. URL: https://www.newsroom.kh.ua/ukraine/sbu-poprosila-pomoshchi-na-kiberfronte (дата звернення: 05.03.2022).

[25] Хакери стверджують, що зламали російські телеканали й показали там бомбардування Харкова. URL: https://tech.liga.net/ua/other/novosti/hakery-utverjdayut-chto-vzlomali-rossiyskie-telekanaly-i-pokazali-tam-bombejku-harkova___(дата звернення: 14.03.2022).

Хакери **Anonymous** дістались Центробанку Росії. Планується що 35000 файлів разом із секретними документами, що їх приховував усіма силами Центробанк, скоро будуть у мережі. Під удар потрапили сайти трьох компаній, що продовжують співпрацю з агресором: мережі гіпермаркетів «**Ашан**»; будівельних гіпермаркетів «**Леруа Мерлен**»; та спортивних товарів **Decathlon**.

Серед іншого Anonymous повалили сайти Нацбанку та Міноборони Білорусі, а також урядовий сайт Чечні. Вони зламали сайт Міноборони Росії і знайшли там ще один доказ безчинства російських окупантів. Йдеться про наказ російським ЗМІ дискредитувати Україну, звинувативши її у жорстокому поводженні з військово-полоненими.

Зокрема, місцевій пресі наказали:

Розробити та поширити серію відеоматеріалів із демонстрацією нелюдської поведінки військовослужбовців Збройних сил України та націоналістичних формувань на території України щодо полонених, які виявили добровільне бажання здатися у полон.

Розробити та поширити серію графічних матеріалів з підтвердженнями фактів використання підставних осіб під час зйомок брифінгів взятих у полон військовослужбовців збройних сил РФ. Також заперечувати факт використання збройними силами РФ військовослужбовців, які проходили термінову службу за призовом.

Здійснити інформаційний супровід у коментарях, основним аргументом використати порушення Женевської конвенції про поводження з військовополоненими.

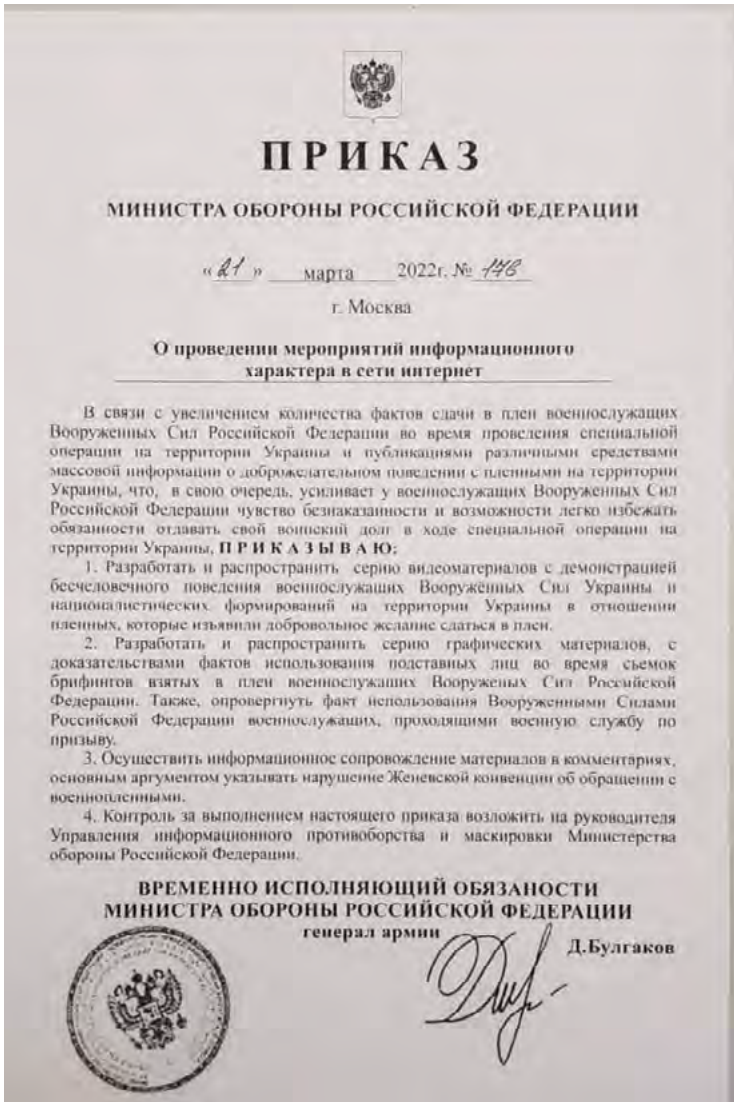
Контролювати виконання такого «наказу» доручили главі Управління інформаційного протиборства та маскування Міністерства оборони РФ [27].

Крім того Anonymous видали в Інтернет інформацію, щодо Наказу Тимчасово виконуючого обов'язки МО РФ генерала армії Д. Булгакова відносно зйомки серії фейкових відео про «українських військовополонених» – рис. 4.

Хакерське угрупу-вання **Anonymous** зламало бази даних Збройних сил Росії та виклало у мережу особисті дані 120 000 російських військових, які беруть активну участь у військових діях в Україні. Про це йдеться у повідомленні групи в Twitter.

«Всі солдати, які беруть участь у вторгненні в Україну, повинні постати перед військовим трибуналом», – йдеться в заяві хакерів.

Звернення до техгігантів. У Мінцифри звернулися до **You Tube, Meta, Netflix, Viber, Pay Pal, Spotify, Apple Music** та інших компаній через вторгнення Росії.



ПРИКАЗ

МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

«21» марта 2022г. № 146

г. Москва

О проведении мероприятий информационного характера в сети интернет

В связи с увеличением количества фактов сдачи в плен военнослужащих Вооруженных Сил Российской Федерации во время проведения специальной операции на территории Украины и публикациями различными средствами массовой информации о доброжелательном поведении с пленными на территории Украины, что, в свою очередь, усиливает у военнослужащих Вооруженных Сил Российской Федерации чувство безнаказанности и возможности легко избежать обязанности отдавать свой воинский долг в ходе специальной операции на территории Украины, **П Р И К А З Ы В А Ю:**

1. Разработать и распространить серию видеоматериалов с демонстрацией бесчеловечного поведения военнослужащих Вооружённых Сил Украины и националистических формирований на территории Украины в отношении пленных, которые изъявили добровольное желание сдаться в плен.

2. Разработать и распространить серию графических материалов, с доказательствами фактов использования подставных лиц во время съемок брифингов взятых в плен военнослужащих Вооруженных Сил Российской Федерации. Также, опровергнуть факт использования Вооруженными Силами Российской Федерации военнослужащих, проходящими военную службу по призыву.

3. Осуществить информационное сопровождение материалов в комментариях, основным аргументом указывать нарушение Женевской конвенции об обращении с военнопленными.

4. Контроль за выполнением настоящего приказа возложить на руководителя Управления информационного противоборства и маскировки Министерства обороны Российской Федерации.

ВРЕМЕННО ИСПОЛНЯЮЩИЙ ОБЯЗАНОСТИ
МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
генерал армии **Д.Булгаков**

Рис. 4. Наказ генерала армії Д. Булгакова

Зокрема Федоров звернувся до: **You Tube** щодо блокування пропагандистських російських ЗМІ, які називаюсь нас «нациками та наркоманами», брешуть та пропагують війну. *У відповідь* YouTube заблокував в Україні канали пропагандистських російських ЗМІ*;*

Meta щодо блокування **Facebook** та **Instagram**. *Цукерберг також відреагував і почав маркувати в інстаграмі сторінки ЗМІ, якими керує Росія. Такі ж мітки з'явилися на сторінках ведучих російських шоу на кшталт Івана Урганта. У* ***Facebook*** взагалі почали блокувати російську пропаганду і надали широкий спектр інструментів для її відслідковування;

Netflix щодо блокування сервісу в Росії.

Міністр пояснив, що у такий спосіб Україна прагне не позбавити росіян доступу до інформації, а достукатися до молоді, проактивного та думаючого населення. Крім того, Мінцифра закликала глобальні цифрові компанії допомогти Україні. У відомстві наголосили, що спільні зусилля можуть зупинити війну проти України.

Звернення до технологічних компаній зі всього світу. Усі цивілізовані країни вже висловили своє занепокоєння та допомогли Україні протистояти російській агресії. Дії технологічних компаній можуть бути значно ефективнішими, щоб швидше зупинити війну в Україні.[26]

Доступ до ресурсів обмежили **Facebook, Twitter та PornHub. Google** вимкнув в Україні можливість відслідковувати трафік на дорогах великих міст в реальному часі.

За результатами засідання **Керівного комітету Спільного центру передового досвіду НАТО з кіберзахисту** Україна буде прийнята до **Спільного центру передового досвіду НАТО** з кіберзахисту як учасник. Представники 27 країн-спонсорів у Керівному комітеті одноголосно підтримали це рішення. Про це йдеться в повідомленні ОКЦ НАТО.

Зазначається, що після того, як Україна направила лист, в якому підтвердила свою зацікавленість у вступі до ОСРТСО НАТО в якості учасника, питання про її членство було поставлено на голосування в Керівному комітеті. «Участь України в роботі Центру посилить обмін кібер-досвідом з іншими країнами-учасницями. Україна може поділитися цінним досвідом з перших рук проти деяких супротивників у сфері кібербезпеки, який може бути використаний для подальших досліджень, освіти та навчання», – сказав полковник **Яак Тарієн**, директор **Спільного центру передового досвіду НАТО з кіберзахисту.**

«Можливості і знання походять з досвіду, і Україна, безумовно, має цінний досвід попередніх кібератак, якими вона може поділитися з OCLTCO НАТО. Естонія, як приймаюча країна ТКОС НАТО, має довгу історію співпраці з Україною у зміцненні її здатності забезпечити кібербезпеку та стійкість, тому ми вітаємо рішення членів ОСРТСО НАТО, які прийняли членство України», – прокоментувала міністр оборони Естонії **Калле Лаанет**.

Міжнародна військова організація зі штаб-квартирою в Таллінні фокусується на проведенні міждисциплінарних прикладних досліджень, консалтингу, підготовки та підготовки фахівців у сфері кібербезпеки.[27] Над Центром НАТО з питань співробітництва у галузі кіберзахисту, поруч з прапорами країн-членів НАТО підняли прапор України.

В Україні почали використовувати штучний інтелект в ході боротьби з вторгненням окупантів з Росії. Пошук проводиться в соцмережах аккаунтів мертвих російських бойовиків. Головне завдання полягає в тому, щоб розвіяти міф про «спецоперацію», на якій немає бійців строкової служби і де ніхто не вмирає.

Сьогодні, 27 квітня 2022 року, понад два місяця початку бойових дій. За цей час фахівці ЗС України нарахували 22,4 тис. військовослужбовців противника вбитими, у ході бойових операцій. 14.03. 2022 в флагман Чорноморського флоту РФ, крейсер «Москва», влучили дві крилаті ракети «Нептун», і він потонув. Перед цим, у порту Бердянська, знищено десантний корабель «Саратов». Крім того з 24 лютого, коли росія розпочала повномасштабну війну проти України, нами знищено понад 940 танків, 2,3 тис. бронемашин та 340 літаків та вертольотів, 1,6 тис. автомобілів з лав ЗС росії.

В той же час в росії це питання замовчується, зі скрипом погоджуються на сотню – другу мертвих російських військовослужбовців. Згідно з інформацією Міноборони росії *«все распространяемые Подоляком якобы «реальные данные» о потерях военной техники и личного состава российских вооруженных сил, в том числе старших и высших офицеров – пропагандистское вранье».*

В Україні вирішили використовувати штучний інтелект, щоб знайти профілі у соцмережах загиблих у війні проти України російських бойовиків, щоб повідомляти про їх смерть рідним. Міністр цифрової трансформації **Михайло Федоров** стверджує «сьогодні ми використовуємо штучний інтелект для пошуку в соціальних мережах акаунтів мертвих російських солдат по фото трупів, щоб повідомити про їхню смерть друзям та близьким, розвіяти міф про «спецоперацію», на якій «немає строковиків» і де «ніхто не вмирає»«. Також міністерство організовує автодозвон в Росію, щоб повідомити родичів про бійців російської армії, що здалися в полон.

Висновки

Продовжується дестабілізація України через кібератаки. На тлі загрози продовження бойових дій це провокує суспільну істерію та б'є по економіці України. Чи є компроміс?

Як відомо, зрештою будь-яка війна закінчується миром, і гібридна – не виняток. Але парадокс у тому, що Росія сама створила ситуацію, за якої майбутній можливий компроміс із НАТО та ЄС тепер вимушено будуватиметься на поверненні до статус-кво. Тобто: відведенні ВМС НАТО із середземноморського регіону та району Чорного моря, а в перспективі – і тих сил, які наразі США тільки готується ввести до Східної Європи для посилення контингенту.

Фактично своєю стратегією Росія досягла протилежної мети та зіштовхнулась не з переляканим Заходом, а з супротивником, який тільки посилився

[26] Цифровий фронт: головні успіхи Мінцифри та української ІТ-Армії у війні з Росією. URL: https://24tv.ua/tsifroviy-front-golovni-uspihi-mintsifri-ukrayinskoyi-it-armiyi_n1883997 (дата звернення: 04.03.2022).

[27] Україну прийняли до однієї зі структур НАТО. URL: https://zn.ua/ukr/WORLD/ukrajinu-prijnjali-do-objednanoho-tsentru-peredovikh-tekhnolohij-z-kiberoboroni-nato.html (дата звернення: 12.03.2022).

біля кордонів Росії. Крім того ведучі бойові дії з РФ необхідно нанести ряд виважених ударів: зруйнувати міст між Кримом і РФ; нанести удари по аеродромах та військовим літакам; портам, базам зберігання озброєння та пального тощо.

При цьому для Кремля різко вимальовуються і контури своїх справжніх ворогів (як то Британія) та латентних союзників (як то Угорщина) у Європі. І питання лише у тому, як самій Україні вигідно скористатися цим блефом століття, в який грає Москва.

Інформація про автора:

Устименко Олександр Володимирович,
кандидат наук з державного управління, старший науковий співробітник,
провідний науковий співробітник науково-дослідного відділу проблем розвитку
інформаційних технологій Центру воєнно-стратегічних досліджень
Національний університет оборони України імені Івана Черняховського
28, Повітрофлотський пр., м. Київ, 03049, Україна

Information about the author:

Ustymenko Oleksandr Volodymyrovych,
Ph.D in Public Administration, Senior Researcher,
Leading Researcher at the Research Department of Information Technology
Development of Center for Military and Strategic Studies
The National University of Defense of Ukraine named after Ivan Chernyakhovsky
28, Povitroflotsky ave., Kyiv, 03049, Ukraine