УДК 351.865(477)
DOI: 10.34132/pard2022.15.02

КІБЕРВІЙНА В УКРАЇНІ ТА ВИКЛИКИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ: КІБЕРНАПАДИ НА ЦИФРОВУ ІНФРАСТРУКТУРУ (ДЕРЖАВНІ УСТАНОВИ, ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ОРГАНІЗАЦІЇ ТРЕТЬОГО СЕКТОРУ)

Бондар Г.Л., канд. політ. наук., доцент, Інститут державного управління, Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна.

◇◇

Стаття присвячена аналізу особливостей реалізації Росією нападів на Україну у кіберпросторі синхронізованими з початком повномасштабного військового вторгнення в країну 24 лютого 2022 року. Проаналізовані виклики (загрози) національній безпеці України у кіберпросторі. Розкрито особливості здійснення кібернападів на цифрову інфраструктуру України зловмисниками, керованими спецслужбами РФ, з метою знищення, порушення або потрапляння у мережі державних установ та об'єкти критичної інфраструктури, для погіршення їх функціонування та для перешкоджання доступу громадян до надійної інформації та життєво важливих послуг. Встановлено, що відомі і підозрювані російські кібергрупи працюють над компрометацією державних та недержавних установ в усіх регіонах України, а використання РФ кібератак, переважно пов'язане з її військовими операціями, спрямованими на служби та установи, які є важливими для цивільного населення. Результати дослідження доводять, що зловмисники використовували шкідливе програмне забезпечення в українських мережах напередодні вторгнення в Україну 24 лютого 2022 року. Висвітлено особливості тісної співпраці урядів, міжнародних об'єднань, технологічних кампаній, фондів з українськими посадовими особами відповідальними за кібербезпеку та співробітниками цих структур, організаціями

та приватними підприємствами для виявлення і усунення загроз українським мережам. Встановлено, що кібератаки, спрямовані на Україну, у тому числі на критично важливу інфраструктуру (державні органи, військовий, енергетичний, промисловий сектор, мобільний та інтернет-зв'язок, ЗМІ та ін.), можуть уразити й інші країни світу, тому підкреслена важливість тісної міжнародної співпраці для запобігання, стримування та реагування на напади у кіберпросторі.

Ключові слова: *кібервійна, кібернапади, цифрова інфраструктура, критична інфраструктура, кібербезпека.*

Постановка проблеми у загальному вигляді. Кібербезпека є важливою складовою національної безпеки України, а захист критичної інфраструктури є одним з пріоритетних напрямків державної політики. Розкриття обсягів, масштабів, методів, можливостей, які використовує РФ в кіберсфері як частини масштабної «гібридної» війни проти України, покликане сприяти поширенню та врахуванню країнами світу українського досвіду боротьби з кібернападами та сприятиме розробці міжнародного скоординованого захисту від кібератак. У звіті компанії Microsoft, оприлюдненому 27 квітня 2022 року, розкрито особливості стратегії, тактики суб'єктів кібернападів, керованих РФ, як форми ведення війни в Україні у кіберпросторі, поєднану з військовим нападом на державу. Деструктивні атаки є компонентом російських кібероперацій під час війни. Кібератаки тривають і загрожують добробуту цивільного населення. Поєднання кібернападів та військового нападу мало на меті порушити функціонування українського уряду та армії, підірвати довіру громадськості до цих інституцій, пошкодити об'єкти критичної інфраструктури, спричинивши незворотні катастрофічні наслідки. Безпекові команди Microsoft, Google, Eset, Fortinet та інших компаній, а також уряди країн світу тісно співпрацюють з українськими посадовими особами з кібербезпеки та співробітниками цих структур, організаціями та приватними підприємствами для виявлення і усунення загроз українським мережам. У січні 2022 року, Центр

розвідки загроз Microsoft виявив шкідливе програмне забезпечення у більш ніж десятках мереж України. Компанія попередила про це український уряд, опублікувала свої висновки, а також встановила безпечні лінії зв'язку з ключовими посадовцями з кібербезпеки в Україні, щоб допомогти українським державним установам, підприємствам та організаціям захиститися від атак. Це включало цілодобовий обмін даними про загрози та розгортання технічних контрзаходів для протидії шкідливому програмному забезпеченню. Оскільки війна триває, а країни світу надають військову допомогу Україні, або вживають санкції проти РФ, ймовірно, що зловмисники, керовані РФ, можуть здійснити кібератаки у відповідь й за межами України. Наразі в Україні триває процес розробки і розвитку власної моделі кіберзахисту держави в умовах протидії російській агресії, з використанням сучасних світових практик, практик країн НАТО та ЄС в означеній сфері. Розробка нових сучасних заходів боротьби з кібернападами українських фахівців та досвід цієї боротьби є нагальним для світової спільноти, оскільки використання кібератак є потужною стратегією дестабілізації та геополітичного впливу країн-агресорів.

Аналіз останніх досліджень і публікацій. Автором статті було проаналізовано звіти та наукові розвідки фахівців передових технологічних та безпекових компаній світу таких, як Microsoft, Google, Eset, Fortinet та ін. щодо кібернападів на стратегічні об'єкти критичної інфраструктури України як нової форми ведення війни РФ у кіберпросторі. Зокрема, спеціальний безпековий звіт компанії Microsoft щодо України, присвячений розкриттю активізації російських кібератак в Україні [1]. Публікації Т. Барта, корпоративного віце-президента компанії Microsoft, щодо гібридної війни в Україні [2], Б. Сміта Президента і віце-голови компанії Microsoft щодо цифрових технологій та війни в Україні [3], Д. Ревея, фахівця з кібербезпеки американської компанії Fortinet, що спеціалізується на пристроях мережевої безпеки [4]. Проаналізовано дослідження від компанії ESET - міжнародного розробника антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки [5]. Проаналізовано заяви щодо кібернападів РФ на Україну від

DOI: 10.34132/pard2022.15.02

міжнародних установ, зокрема від Ради Європи Європейського Союзу [6]. Проаналізовано виступи 21 червня 2022 року на засіданні Ради Безпеки ООН, присвяченому Україні щодо попередження розпалювання расової та релігійної ворожнечі, яке може спровокувати жорстокість злочинів та юридичного зобов'язання держав запобігати геноциду. Зокрема, виступ Д. Коена, голови компанії Jigsaw, яка входить до складу Google, щодо небезпек використання цифрових засобів у веденні війни, їх неконтрольованості та розробки нагальних законодавчих змін для запобігання цим загрозам [7]. У статті В. Ємельянова та Г. Бондар наведено приклади кібернападів, з використанням шкідливих програм, у період з грудня 2015 року по грудень 2016 року в Україні, які мають схожі ознаки з нападами на об'єкти критичної інфраструктури у 2022 році [8]. Проаналізовано обвинувальний акт уряду США (Департаменту юстиції) від 2020 року у якому шістьом офіцерам російського ГРУ висунули звинувачення у розгортанні зловмисного програмного забезпечення та інших руйнівних дій у кіберпросторі по всьому світу [9]. Було праналізовано статтю американського видання The Economist щодо подолання проблеми з відключенням інтернет-зв'язку в Україні під час війни засобами компанії І. Маска – «SpaceX», через доступ до широкосмугового інтернету, завдяки «Starlink» [10]. Також використовувались дані щодо атак, а також щодо світової співпраці у безпековій, гуманітарній, фінансовій сферах з офіційних сайтів органів державної влади.

Формулювання цілей статті (постановка завдання)**.** Під час дослідження автором були визначені наступні завдання:

– проаналізувати особливості стратегії, методи та масштаби нападу на цифрову інфраструктуру України, державні установи, стратегічні об'єкти критичної інфраструктури, організації третього сектору кіберсуб'єктів, керованих РФ як частини масштабної «гібридної» війни проти України;

– проаналізувати виклики (загрози) національній безпеці України у кіберпросторі;

– розкрити особливості співпраці урядів, міжнародних об'єднань, технологічних кампаній, фондів з українськими посадовими

особами відповідальними за кібербезпеку та співробітниками цих структур, організаціями та приватними підприємствами для виявлення і усунення загроз українським мережам.

Виклад основного матеріалу дослідження. У звіті компанії Microsoft, оприлюдненому 27 квітня 2022 року [1], проаналізована кіберактивність суб'єктів нападу, яка є частиною війни в Україні. Висвітлено роботу кампанії у співпраці з українськими посадовими особами з кібербезпеки та представниками приватного сектору, які забезпечують захист від кібератак. Постійний щоденний моніторинг Microsoft свідчить про те, що російський напад на Україну у кіберсфері мав руйнівні наслідки. Метою формування та оприлюднення звіту компанії Microsoft було розкриття обсягів, масштабів, методів, можливостей, які використовує РФ в кіберсфері як частини масштабної «гібридної» війни проти України, також відзначено роботу організацій в Україні, які протидіяли цьому. Також цей звіт є важливим для врахування організаціями у всьому світі стратегічних рекомендацій компанії Microsoft.

Протягом військового конфлікту компанія Microsoft спостерігала з боку Росії поєднання кібернападів з військовими діями проти України. Щонайменше шість російських суб'єктів Advanced Persistent Threat (APT) провели понад 237 деструктивних атак, шпигунських операцій в той самий час, коли російські війська атакували Україну з суші, повітря та моря. Ці атаки тривають і загрожують добробуту цивільного населення. Поєднання кібернападів та військового нападу мало на меті порушити функціонування українського уряду та армії і підірвати довіру громадськості до цих інституцій. Деструктивні атаки були помітним компонентом російських кібероперацій під час війни.

За день до військового вторгнення оператори пов'язані з ГРУ, російською військовою розвідкою здійснили деструктивні атаки на сотні систем українського уряду, IT сектору, енергетичних та фінансових організацій. Діяльність, яку спостерігала компанія Microsoft, включала в себе спроби зловмисників знищити, порушити або потрапити в мережі державних установ, та об'єкти критичної інфраструктури, на деякі з них російські збройні сили одночасно здійс-

DOI: 10.34132/pard2022.15.02

нили наземні атаки та ракетні удари. Ці мережеві операції повинні були не лише погіршити функції установ, на які вони були спрямовані, а й перешкодити доступу громадян до надійної інформації та життєво важливих послуг, похитнути довіру до керівництва країни. На думку фахівців компанії Microsoft, якщо враховувати ці дії як російські військові цілі в інформаційній війні, то вочевидь вони були спрямовані на підрив політичної волі України і здатності продовжувати боротьбу, полегшуючи при цьому збір розвідувальних даних, які могли б забезпечити тактичні або стратегічні переваги російським військам [1, С. 2].

Безпекові команди Microsoft тісно співпрацюють з українськими посадовими особами з кібербезпеки та співробітниками цих структур, організаціями та приватними підприємствами для виявлення і усунення загроз українським мережам. У січні 2022 року, Центр розвідки загроз Microsoft (Microsoft Threat Intelligence Center - MSTIC) виявив шкідливе програмне забезпечення у більш ніж десятках мереж України. Компанія попередила про це український уряд та опублікувала свої висновки. Після цього інциденту Microsoft встановив безпечні лінії зв'язку з ключовими посадовцями з кібербезпеки в Україні, щоб допомогти українським державним установам, підприємствам та організаціям захиститися від атак. Це включало цілодобовий обмін даними про загрози та розгортання технічних контрзаходів для протидії шкідливому програмному забезпеченню.

Така цілеспрямована співпраця компанії Microsoft, у поєднанні з її унікальним баченням постраждалих систем, висвітлила російські кіберцілі, тактику та процедури, а також нею було надано пропозиції щодо захисту мереж користувачів, які втягнуті у військовий конфлікт. За спостереженнями Microsoft, «відомі і підозрювані російські державні суб'єкти (Russian nation-state actors) працюють над компрометацією установ в усіх регіонах України» [2].

Використання Росією кібератак, переважно пов'язане з її військовими операціями, спрямованими на служби та установи, які є важливими для цивільного населення. Наприклад, 1 березня 2022

року російський зловмисник здійснив кібератаки на велику телерадіокомпанію, а того ж дня російські військові оголосили про намір знищити українські «дезінформаційні» цілі та завдали ракетного удару по телевежі в Києві [1, С. 12].

13 березня 2022 року, протягом третього тижня вторгнення, інша російська кібергрупа вкрала дані у організації з ядерної безпеки через кілька тижнів після того, як російські військові підрозділи почали захоплювати атомні електростанції, що викликало занепокоєння щодо радіаційного опромінення та катастрофічних наслідків аварій. Поки російські війська окуповували місто Маріуполь, українці почали отримувати на електронну пошту листи від російського зловмисника, який видавав себе за жителя Маріуполя, й неправдиво звинувачував український уряд у тому, що він «кинув» громадян України напризволяще [2].

Деструктивних атак, які відслідковувала компанія Microsoft нараховувалось близько 40, вони були спрямовані на сотні систем та викликали особливе занепокоєння, оскільки 32% деструктивних атак були спрямовані безпосередньо на українські урядові організації на національному, регіональному та місцевому рівнях. Понад 40% деструктивних атак були спрямовані на організації, які відносяться до об'єктів критичної інфраструктури, також це стосувалось негативного впливу на український уряд, військових, економіку та цивільне населення [1, С. 4].

Кіберзлочинці використовують різноманітні методи отримання початкового доступу до своїх цілей, реалізуючи фішингові кампанії, використовуючи невиправлені вразливості локальних серверів Exchange і компрометацію постачальників ІТ-послуг. Цей початковий доступ дозволяє їм проводити операції зі знищення, вилучення даних, а також для довготривалого шпигунства та спостереження. Зловмисники часто змінюють своє шкідливе програмне забезпечення під час кожного застосування, щоб уникнути виявлення. У звіті компанії Microsoft надано інформацію про атаки зловмисного програмного забезпечення - **wiper**.

Термін **wiper** походить від його основної функції, коли метою зловмисного програмного забезпечення є стирання жорсткого диску

DOI: 10.34132/pard2022.15.02

машини-жертви, знищення даних [4]. Зазвичай його використовують для фінансової вигоди, знищення доказів, саботажу і кібервійни, для шпигунства, знищення слідів та всіх доказів атаки на організації. Wiper не тільки стирає докази, оскільки зазвичай, масштаби знищення даних змушують фахівців з кібербезпеки зосередитися на відновленні даних та операцій, а не на розслідуванні вторгнення.

Станом на 28 квітня 2022 року було виявлено сім різних атак шкідливого програмного забезпечення wiper (WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AcidRain), спрямованих на українську інфраструктуру, або українські компанії. Усі атаковані цілі відповідають інтересам Росії в російсько-українській війні. Метою атаки могло бути пошкодження критичної інфраструктури для того, щоб викликати хаос і посилити психологічний тиск на противника, або спровокувати руйнування тактичної цілі, що має свою цінність у війні. Шкідливе програмне забезпечення AcidRain wiper було використане під час атаки на постачальника послуг супутникового широкосмугового доступу **Viasat KA-SAT**. Зловмисники отримали доступ до інфраструктури управління провайдера для розгортання AcidRain на модемах KA-SAT, які використовуються в Україні [4].

Європейський Союз разом із міжнародними партнерами засудили зловмисну кіберактивність Російської Федерації проти України, спрямовану на супутникову мережу KA-SAT, що належить Viasat [6]. Ця кібератака сталася за годину до військового вторгнення Росії в Україну 24 лютого 2022 року. Ця кібератака мала значний вплив, спричинивши невибіркову втрату зв'язку та збої в роботі кількох державних органів, підприємств та користувачів в Україні, а також вплинула на декілька держав-членів ЄС. «Кібератаки, спрямовані на Україну, у тому числі на критично важливу інфраструктуру, можуть уразити й інші країни та спричинити системні наслідки, що загрожують безпеці громадян Європи. Європейський Союз, співпрацюючи зі своїми партнерами, розглядає подальші кроки для запобігання, стримування та реагування на таку шкідливу поведінку у кіберпросторі» [6]. Європейський Союз наголосив, що й надалі надаватиме скоординовану політичну, фінансову та матеріальну

підтримку Україні для посилення її кіберстійкості. «Росія повинна припинити цю війну і негайно покласти край безглуздим людським стражданням» [6].

«Групи зловмисників, відомі своїми зв'язками з ГРУ чи такі, що підозрюються в цьому, постійно розробляли і використовували деструктивне шкідливе програмне забезпечення wiper або подібні деструктивні інструменти для цільових українських мереж з частотою два-три інциденти на тиждень напередодні вторгнення в Україну 24 лютого 2022 року. З 23 лютого по 8 квітня 2022 року компанія Microsoft зафіксувала майже 40 розрізнених деструктивних атак, які постійно знищували файли в сотнях систем у десятках організацій в Україні» [1, С. 3]. Дані зі звіту компанії Microsoft доводять, що у перший тиждень (23 лютого-2 березня) нападу РФ на Україну було зафіксовано 22 деструктивних інциденти; другого тижня (3-9 березня) не було кіберінцидентів; третього тижня (10-16 березня) деструктивних інцидентів було 4; четвертого тижня (17-23 березня) – 6 деструктивних інциденти; 5 тижня (24-30 березня) – 3 інциденти; шостого тижня (31 березня – 8 квітня) - 2 деструктивних інциденти [1, С. 4].

Microsoft фіксує, що пов'язані з Росією злочинні угруповання, раніше вже використовувались для нападу ще у березні 2021 року, коли вони періодично нападали на Україну і реалізовували руйнівні заходи проти організацій всередині країни, і проти її союзників. Microsoft поки не береться стверджувати про рівень координації між різними злочинними угрупованнями, але їхня спільна діяльність виявилася спрямованою на забезпечення постійного доступу для збирання стратегічної та бойової розвідувальної інформації, або для сприяння майбутнім руйнівним нападам на Україну під час війни (Див. рис.1).

На схемі Microsoft визначено російських суб'єктів кіберзагроз пов'язаних з Головним розвідувальним управлінням (ГРУ), Федеральною службою безпеки (ФСБ), Службою зовнішньої розвідки (СЗР) РФ, за якими спостерігав Центр розвідки загроз Microsoft (MSTIC). Зокрема за тим, які саме зловмисники реалізовували операції, та на які українські об'єкти вони були спрямовані перед вторг-

DOI: 10.34132/pard2022.15.02

ненням. На початку 2021 року, коли російські війська вперше почали масований рух до кордону з Україною, були визначені їхні цілі для кібератак, вони стосувалися отримання інформації про військове та закордонне партнерство України. Зокрема, російська група **NOBELIUM** розпочала масштабну фішингову кампанію проти українських зусиль щодо залучення міжнародної підтримки проти дій Росії. Аналогічно, **DEV-0257** (відомий як Ghostwriter) запустив фішингові кампанії, намагаючись отримати доступ до електронних акаунтів та мереж українських військових [1, С. 6].

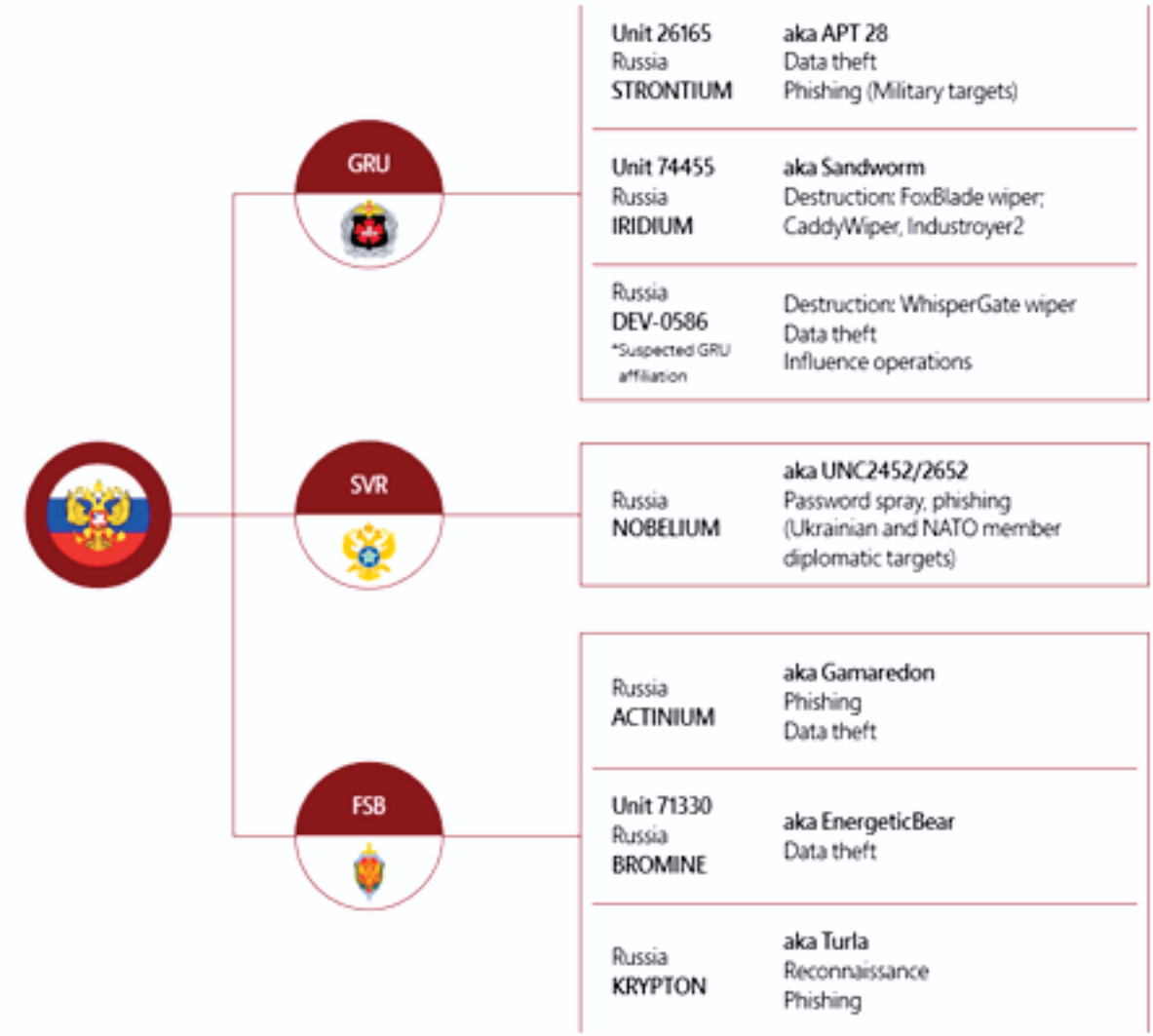


Рис. 1. Російські злочинні кіберугруповання

Джерело: [1]

Варто зазначити, що російські суб'єкти атакуючи мережі в Україні та країнах-партнерах, позиціонували себе як суб'єкти третьої сторони. До середини 2021 року компанія Microsoft фіксувала відомих і підозрюваних російських зловмисників, які створювали загрози, спрямовані на постачальників у ланцюгу поставок в Україні та за кордоном, для отримання інформації про їхнє місце знаходження. Також атаки спрямовувались проти партнерів України, країн-членів НАТО. **DEV-0586**, раніше невідома група з підозрілими російськими військовими зв'язками, скомпрометувала мережу ІТ-компанії, яка розробила системи управління ресурсами для Міністерства оборони України та установ зв'язку і транспортного сектору.

NOBELIUM намагався отримати доступ до ІТ-компаній, у яких клієнти - це уряди, переважно країн-членів НАТО. Вони успішно скомпрометували компанії, а потім використовували привілейовані облікові записи з метою зламу та крадіжки даних про зовнішню політику установ Заходу. Ці традиційні шпигунські операції мали на меті отримання доступу до зовнішньополітичних цілей організацій країн-членів НАТО. Вони могли надати російському керівництву постійну інформацію про те чого очікувати від Заходу у відповідь на дії Росії в Україні. Приблизно 93% усіх скерованих Росією нападів протягом 2021 року, що спостерігались компанією Microsoft, були спрямовані на країни-члени НАТО, зокрема проти Сполучених Штатів, Великобританії, Норвегії, Німеччини та Туреччини.

Російські суб'єкти атак постійно шукали доступ до інформації про військові та гуманітарні можливості України. У 2021 році було зафіксовано кіберзагрози від російських спецслужб, спрямовані на Україну, для спостереження або компрометації установ, які могли б надати цінні данні розвідці РФ про українських військових, а також про дипломатичні чи гуманітарні заходи на військові дії. **ACTINIUM** запустив фішингові кампанії в Україні для отримання доступу до акаунтів іноземних військових радників та гуманітарних працівників у серпні 2021 року. Приблизно в той же час **STRONTIUM** спробував скомпрометувати оборонні установи в Україні. **ACTINIUM, NOBELIUM, BROMINE, SEABORGIUM і**

DOI: 10.34132/pard2022.15.02

DEV-0257 шукали постійний доступ до бази даних української оборони, оборонної промисловості, зовнішньої політики, національного та місцевого управління, правоохоронних та гуманітарних установ [1, С. 6].

Для кіберзлочинців, пов'язаних з РФ важливим був доступ до критичної інфраструктури України для її майбутнього руйнування. Зловмисники також встановили доступ і присутність в мережах для майбутніх деструктивних атак. Наприкінці 2021 року підозрювані російські кіберактори, які так себе позиціонували в мережах, здійснили деструктивні атаки на українських постачальників ресурсів для енергетичного сектору та IT провайдерів, включаючи **Kitsoft** (постачальника IT-послуг). DEV-0586 скомпрометувало Kitsoft, щоб полегшити знищення в мережах кількох її клієнтів у січні 2022 року.

Нижче наводиться діаграма найбільш атакованих країн зловмисниками з інших країн (не тільки з РФ), за даними компанії Microsoft (липень 2020-червень 2021 рр.) (Див. рис.2) [1, С. 6].

У діаграмі від компанії Microsoft станом на червень 2021 року Україна була другою країною, яка постраждала від нападів. 19% усіх повідомлень про загрози для України, які Microsoft надала протягом зазначеного періоду, переважно стосувались збільшення російської активності. Деструктивні атаки, зафіксовані компанією Microsoft, свідчили про майбутнє неминуче вторгнення.

На початку 2022 року, коли дипломатичними зусиллями не вдалося уникнути ескалації напруженості навколо нарощування сил російської армії біля кордонів України, також збільшилась інтенсивність кібератак на українські установи. На початку січня 2022 року DEV-0586 запустив шкідливе програмне забезпечення (WhisperGate5), яке шукало та видаляло вибрані розширення файлів, а потім маніпулювало основним завантажувальним записом (MBR) та робило атаковані прилади непрацездатними. Це руйнівне шкідливе програмне забезпечення вплинуло на державні системи та IT-сектор, що в поєднанні зі зламом українських урядових веб-сайтів у лютому, мало бути попередженням, спрямованим на спонукання українців до поступок (Див. рис. 3) [1, С. 7].

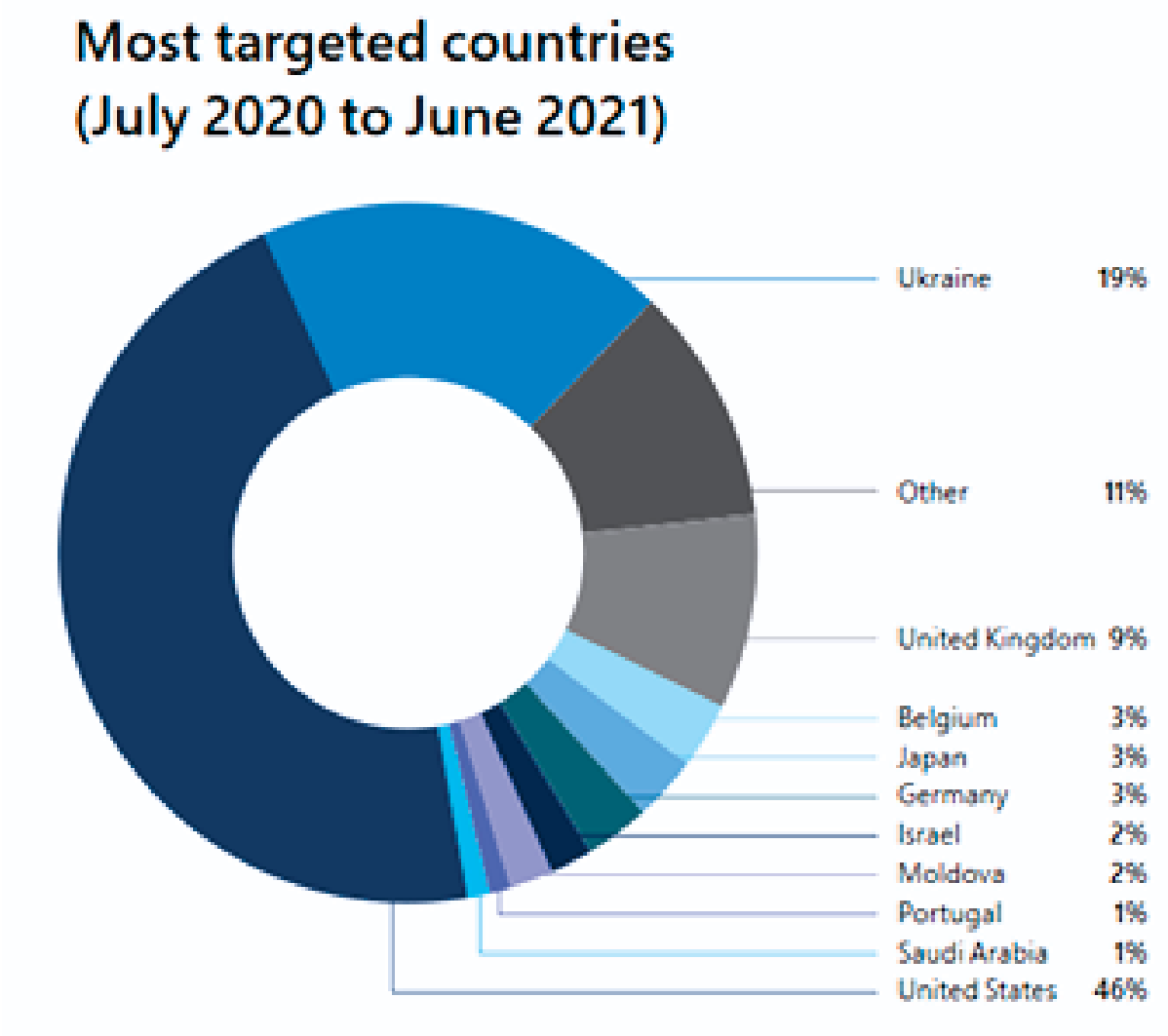


Рис. 2. Найбільш атаковані країни кіберзлочинцями станом на липень 2020-червень 2021 рр.

Джерело: [1, С. 6].

Хронологія подій перед вторгненням свідчить про те, що російські загрози стали більш руйнівніми, а найбільші помітні кібератаки проти України спостерігаються після великих дипломатичних невдач РФ пов'язаних з воєнним конфліктом. Кібератаки, зокрема, було здійснено напередодні російського вторгнення 24 лютого 2022 року, коли IRIDIUM запустив FoxBlade6 (він же HermeticWiper) шкідливе програмне забезпечення для знищення приблизно 300 систем у понад десятка державних установ, IT, енергетичного, аграрного та фінансового секторів в Україні.

DOI: 10.34132/pard2022.15.02

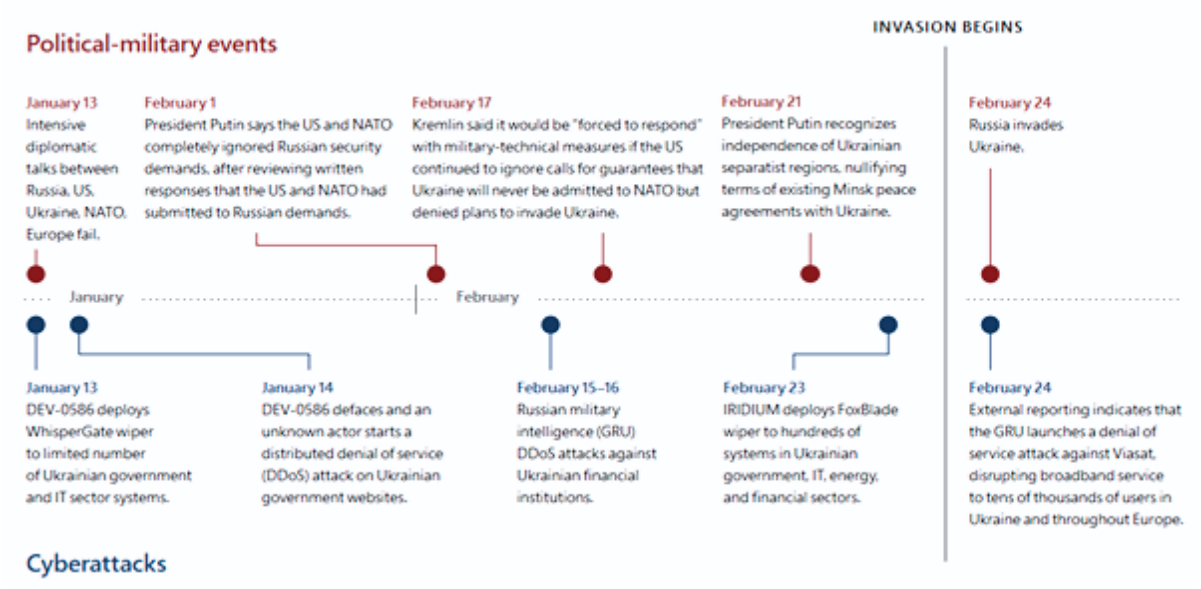


Рис. 3. Зв'язок військово-політичних подій з кібератаками РФ у 2022 році

Джерело: [1, С. 7]

Після запуску FoxBlade6 швидко поширюється і здатен впливати на всі приєднані до домену пристрої атакованої установи. Синхронізація військових ударів і кібернападів доводить зв'язок операцій в комп'ютерних мережах і військових операцій. Відповідно, кібероперації до цього часу узгоджувалися з діями щодо знищення, або дискредитації українського уряду, військових та економічних функцій держави, впливу на критичну інфраструктуру, та зменшення доступу української громадськості до інформації (Див. рис. 4) [1, С. 8].

Компанія Microsoft безпосередньо взаємодіяла з ураженими суб'єктами в Україні та спостерігала, що кібероперації та військові операції, були спрямовані на одні й ті самі військові цілі. Групи кіберзлочинців, поширюючи загрози, часто обирали саме ті сектори або географічні місця й приблизно в той же час, що їх обирали для нападу й російські війська. (Див. рис. 5) [1, С.10].

Під час ведення РФ військових дій та одночасної реалізації ними кібернападів на Україну, фахівці компанії Microsoft фіксували цю системність, здійснюючи щотижневу постійну аналітичну роботу (Див. рис. 6).

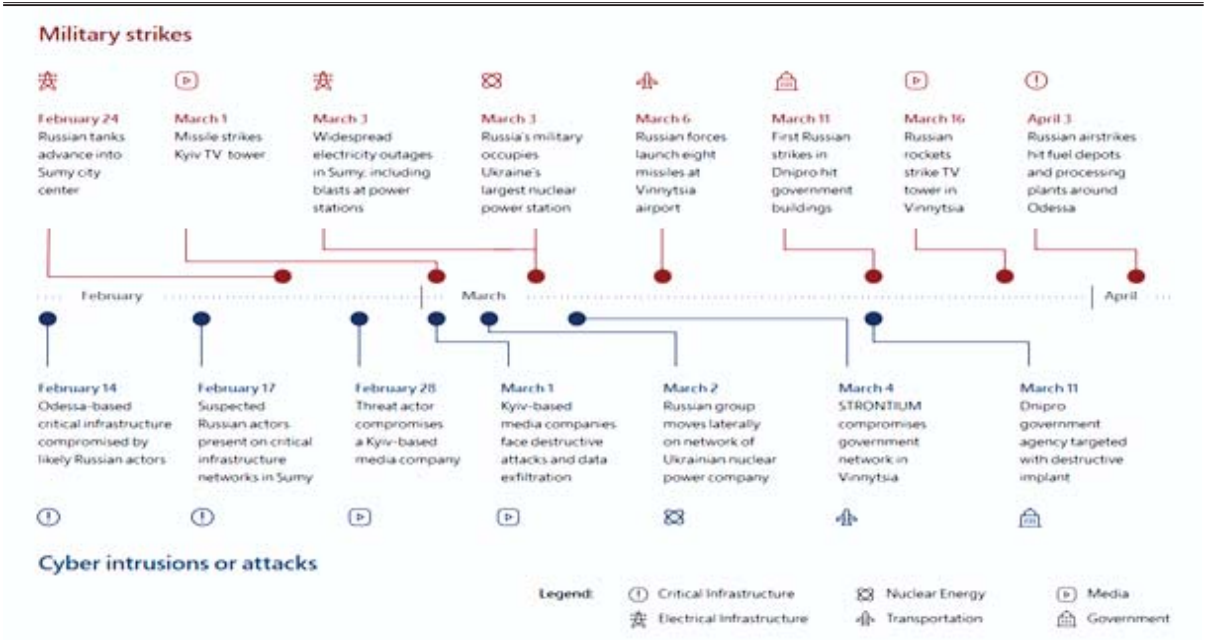


Рис. 4. Синхронізація військового нападу на Україну та кібератак російських зловмисників

Джерело: [1, С. 8]

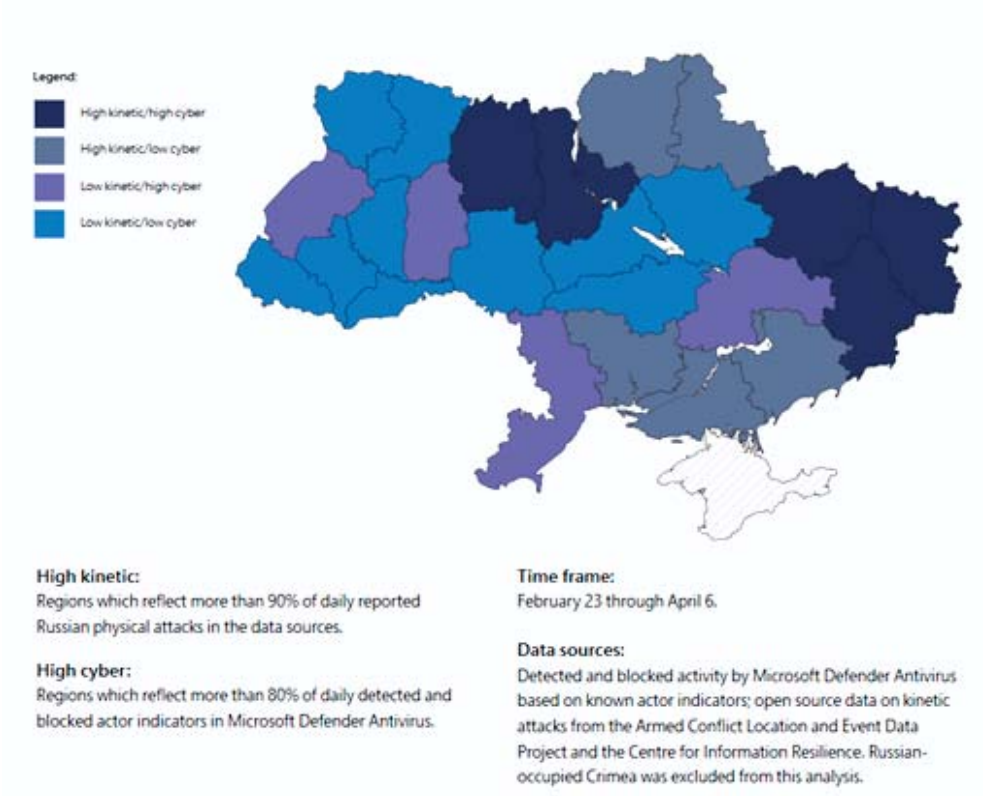


Рис. 5. Карта військових дій та кіберактивності РФ з 23 лютого по 6 квітня 2022 року

DOI: 10.34132/pard2022.15.02

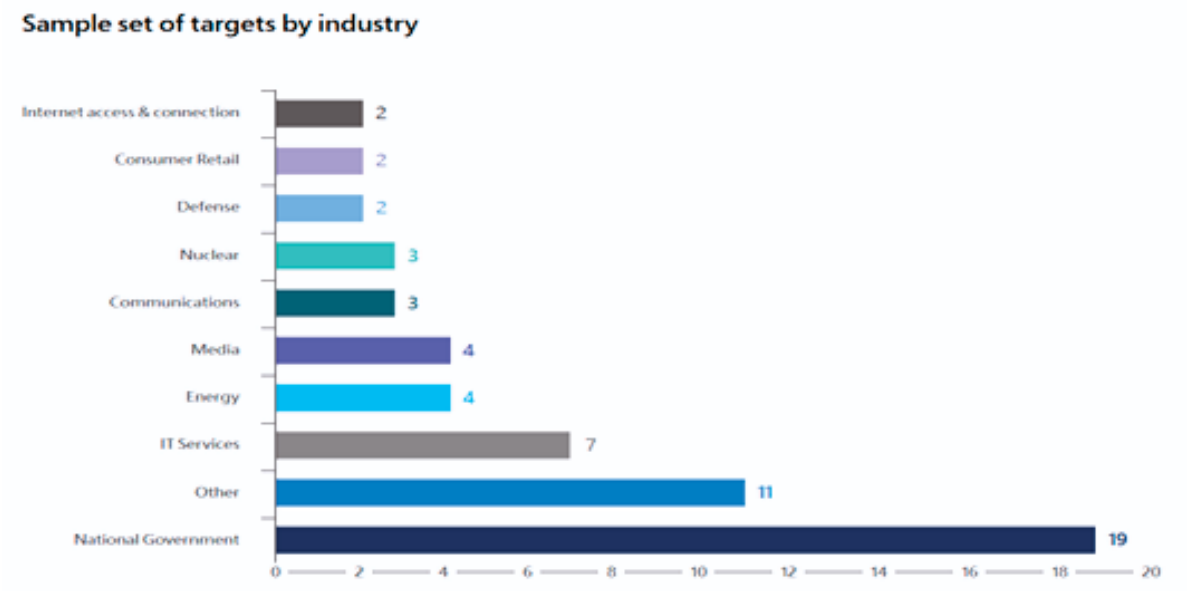


Рис. 6. Цілі кібернападів на Україну за галузями

Джерело: [1, С. 11]

На наведеній діаграмі визначено перелік галузей, які постраждали від керованих РФ вторгнень у мережу, або деструктивних атак під час російського нападу на Україну. Національні урядові установи та об'єкти критичної інфраструктури були головними цілями. До категорії «Інше» віднесено 11 інших постраждалих установ, зокрема, регіональні та місцеві органи влади, сільське господарство, оборонно-промисловий комплекс, охорону здоров'я, транспорт та фінанси та ін.

У перший тиждень війни (**23 лютого – 2** березня), підозрювані у контролі з РФ кіберзлочинці, та російські війська від початку повномасштабного вторгнення намагалися контролювати інформаційне середовище в Україні. Протягом першого тижня вторгнення в Україну, російська кібергрупа **DesertBlade** атакувала телерадіокомпанію 1 березня, того ж дня російські військові оголосили про свій намір знищити «дезінформаційні» цілі в Україні та скерували ракетний удар по телевежі в Києві. Метою нападів було знищення головного джерела інформації для української громадськості [1, С. 12]. Інститут звітності про війну та мир (IWPR), зафіксував, що 27 лютого російські війська, захопивши місто Бердянськ, одразу оку-

пували телевежу і вимкнули всі трансляції. Це довело, що встановлення інформаційного контролю за трансляцією – це одна з найважливіших військових та кіберцілей РФ. Спроби компрометації та/або запуску шкідливого програмного забезпечення у медіакампаніях спостерігається протягом всієї війни.

Російська злочинна кібергрупа **IRIDIUM** реалізовувала операції проти української економіки, відповідно до російських військових цілей, щоб її знищити. **IRIDIUM** впровадив шифрувальник файлів у мережу сільськогосподарської фірми для нанесення їй шкоди в подальшому. Microsoft припускає, що метою атаки було виробництво зерна, основного експортного товару в економіці України. На початку квітня 2022 року Світовий банк передбачав, що війна в Україні призведе до падіння її економіки до 45,1%, частково за рахунок руйнування інфраструктури і припинення імпорту та експорту [1, С.12].

На початку другого тижня війни (**3-9 березня**), російські війська готувалися до наступу на Київ. У той же час відомі і підозрювані у зв'язках з РФ кібергрупи намагалися скомпрометувати джерела публічної інформації та інфраструктуру зв'язку, й вплинути на українські військові операції.

Також однією з цілей зловмисників була компрометація систем цифрових медіа. **DEV-0257** і **STRONTIUM** шукали доступ до військових та регіональних державних облікових записів, шляхом запуску фішингової кампанії проти українських військових і працівників уряду. Регіональні органи влади були новими цілями для STRONTIUM, оскільки він зазвичай атакував державні установи загальнонаціонального рівня [1, С. 13].

Третього тижня від початку повносштабного вторгнення в Україну (**10-16 березня**), війська РФ захопили АЕС. Одночасно з цими діями російські військові та державні ЗМІ поширювали дезінформацію про те, що Україна нібито працювала над створенням хімічної та біологічної зброї, а кібергрупи, пов'язані з РФ, у відповідь реалізовували операції щодо крадіжки даних з установ ядерного сектору, що й мало на меті припинити вищезгадані «загрозливі» дії України [1, С. 14].

DOI: 10.34132/pard2022.15.02

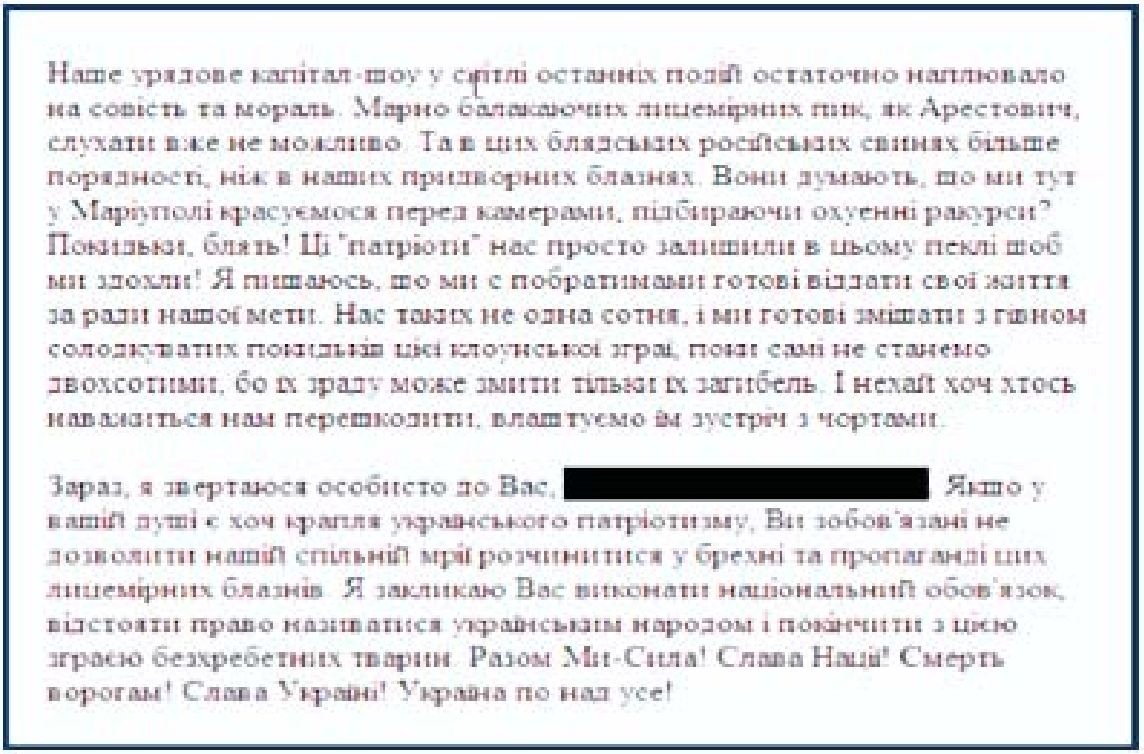
17-23 березня (четвертий тиждень) кіберзлочинці атакували логістичні центри та регіональні державні установи, одночасно з оголошенням РФ про стратегічне перефокусування її військ з Київського напрямку на Схід України. **IRIDIUM** здійснив деструктивну атаку на мережу постачальника транспортних/логістичних послуг, який брав участь у переміщенні українського постачання в гарячі воєнні точки. Штаб-квартира фірми розміщена в Західній Україні, куди надходить значна частина іноземної військової та гуманітарної допомоги. За тиждень до цього підозрювана російська кібергрупа видалила дані регіональної державної мережі на сході України, порушивши процес надання там державних послуг [1, С. 14].

Протягом п'ятого тижня (**24-30 березня**), підозрювані російські кібергрупи, обрали за мету для нападу українські організації громадської підтримки та сектор комунікацій, під час переговорів про мир між РФ та Україною в Туреччині, для обговорення резолюції щодо припинення війни. Невідомі кіберсуб'єкти скомпрометували та знищили дані на порталі, який з'єднує громадян з урядовими послугами і скомпрометували мережу великого медіа. Окремо українська влада повідомила, що вона знищила п'ять «ворожих» ботоферм, які поширювали дезінформацію про російське вторгнення в українському публічному просторі з 24 лютого [1, С. 14].

Компанія Microsoft помітила спроби підозрюваних у зв'язках з РФ суб'єктів посилити привілеї в мережі провайдера інтернет-зв'язку та розширити свої цілі через спроби скомпрометувати провайдера мобільного зв'язку. Окремо Forbes повідомив, що найбільший в Україні провайдер телекомунікацій Укртелеком зазнав серйозної кібератаки, яка, як стверджує NetBlocks, призвела до падіння обслуговування до 13% від довоєнного рівня. Таким чином, серед інших цілей атак були й дані сектору зв'язку [1, С. 14].

На шостому тижні провномасштабного вторгнення в Україну (**31 березня – 8 квітня**), спостерігалась ескалація атак на енергетичну інфраструктуру та зафіксовано спроби вплинути на підтримку українцями свого уряду. **IRIDIUM** і підозрювані російські кібергрупи здійснили вторгнення в мережу української енергетичної компанії ще до початку вторгнення. За цей час IRIDIUM підготував

запуск деструктивної атаки на мережу регіонального постачальника енергії. Тим часом **DEV-0586** запустив кібероперацію з метою налаштування громадян України проти свого уряду. DEV-0586 надсилав електронні листи, маскуючись під мешканця оточеного Маріуполю, звинувативши українську владу у відмові від своїх грмадян, запропонувавши чинити опір владі. У фішинговому повідомленні не було шкідливих посилань чи вкладень. Відповідно метою операції був вплив на українських громадян. Це перший зафіксований випадок інтенсивних антивладних повідомлень, надісланих на електронну пошту. Нижче наводиться знімок екрана повідомлення електронної пошти DEV-0586 до громадян України, наданий у звіті Microsoft. При написанні повідомлення зловмисниками було застосовано машинний переклад (Див. рис. 7) [1, С.15].



Наше урядове капітал-шоу у світлі останніх подій остаточно наплювало на совість та мораль. Марно балакаючих лицемірних пик, як Арестович, слухати вже не можливо. Та в цих блядських російських свинях більше порядності, ніж в наших придворних блазнях. Вони думають, що ми тут у Маріуполі красуємося перед камерами, підбираючи охуенні ракурси? Покидьки, блять! Ці "патріоти" нас просто залишили в цьому пеклі щоб ми здохли! Я пишаюсь, що ми є побратимами готові віддати свої життя за ради нашої мети. Нас таких не одна сотня, і ми готові змішати з гівном солодкуватих покидьків цієї клоунської зграї, поки самі не станемо двохсотими, бо їх зраду може змити тільки їх загибель. І нехай хоч хтось наважиться нам перешкодити, влаштуємо їм зустріч з чортами.

Зараз, я звертаюся особисто до Вас, [redacted]. Якщо у вашій душі є хоч крапля українського патріотизму, Ви зобов'язані не дозволити нашій спільній мрії розчинитися у брехні та пропаганді цих лицемірних блазнів. Я закликаю Вас виконати національний обов'язок, відстояти право називатися українським народом і покінчити з цією зграєю безхребетних тварин. Разом Ми-Сила! Слава Нації! Смерть ворогам! Слава Україні! Україна по над усе!

Рис. 7. Фішингове повідомлення жителям Маріуполя від зловмисників - DEV-0586

Повідомлення були адресовані конкретним людям, і при зверненні були використані їхні справжні імена, що, на думку фахівців Microsoft, підвищує ймовірність того, що DEV-0586 викрали

DOI: 10.34132/pard2022.15.02

цю персональну інформацію принаймні в однієї зі своїх урядових жертв.

За прогнозами фахівців Microsoft, триваючі руйнівні кібератаки в Україні можуть бути ще більш тяжкими за наслідками, в тому числі нести загрози й для глобальної кібербезпеки. Зберігається небезпека використання злочинними кібергрупами таких можливостей для нападу як **zero-days** (невідома вразливість програмного забезпечення), атаки на критичну інфраструктуру, атаки на ланцюги постачання та інші нові методи в середньостроковій перспективі.

Велика безпекова спільнота, разом з Microsoft, чисельністю сягає за межі України. Ця спільнота прагне й надалі виявляти і пом'якшувати раніше невідомі вразливості та ланцюги атак, змушуючи диверсифіковану екосистему, з добре забезпеченими кіберсуб'єктами, закривати вразливості і перешкоджати здійсненню «**N-day attacks**». Організації у всьому світі повинні визнати і підготуватися до реальності, що такі дії будуть відбуватися і навряд чи будуть обмежені певним доменом.

Під час складання звіту Microsoft та кібербезпекова компанія ESET співпрацювали з українською владою для виявлення та пом'якшення впливу атаки **IRIDIUM wiper** на інфраструктуру, зокрема, на систему управління промисловістю (Industrial Control System (ICS)) української енергетичної компанії [5]. Компанія **ESET** у співпраці з **CERT-UA** проаналізували атаку проти української енергетичної кампанії, яка відбулася 8 квітня 2022 року, та встановили, що вона планувалася за два тижні до цієї дати. Під час нападу використовувалось шкідливе програмне забезпечення з підтримкою ICS і wiper для стирання диску в операційних системах Windows, Linux і Solaris. На думку фахівців компанії ESET, зловмисники використали нову версію шкідливого програмного забезпечення **Industroyer - Industroyer2**, яке використовувалося у 2016 році для відключення електроенергії в Україні. Відповідальною за цю атаку є група **Sandworm**. Зловмисники Sandworm спробували розгорнути шкідливе програмне забезпечення **Industroyer2** на високовольтних електропідстанціях в Україні. Разом з Industroyer2, Sandworm використовував ще кілька руйнівних шкідливих програм, включаючи

CaddyWiper, ORCSHRED, SOLOSHRED і AWFULSHRED. На даний момент невідомо, як саме зловмисники скомпрометували початкову жертву, а також як вони перейшли з IT-мережі до мережі системи управління промисловістю (Industrial Control System (ICS). Нижче наведено огляд використаних під час нападу шкідливих програм (Див. рис. 8) [5].

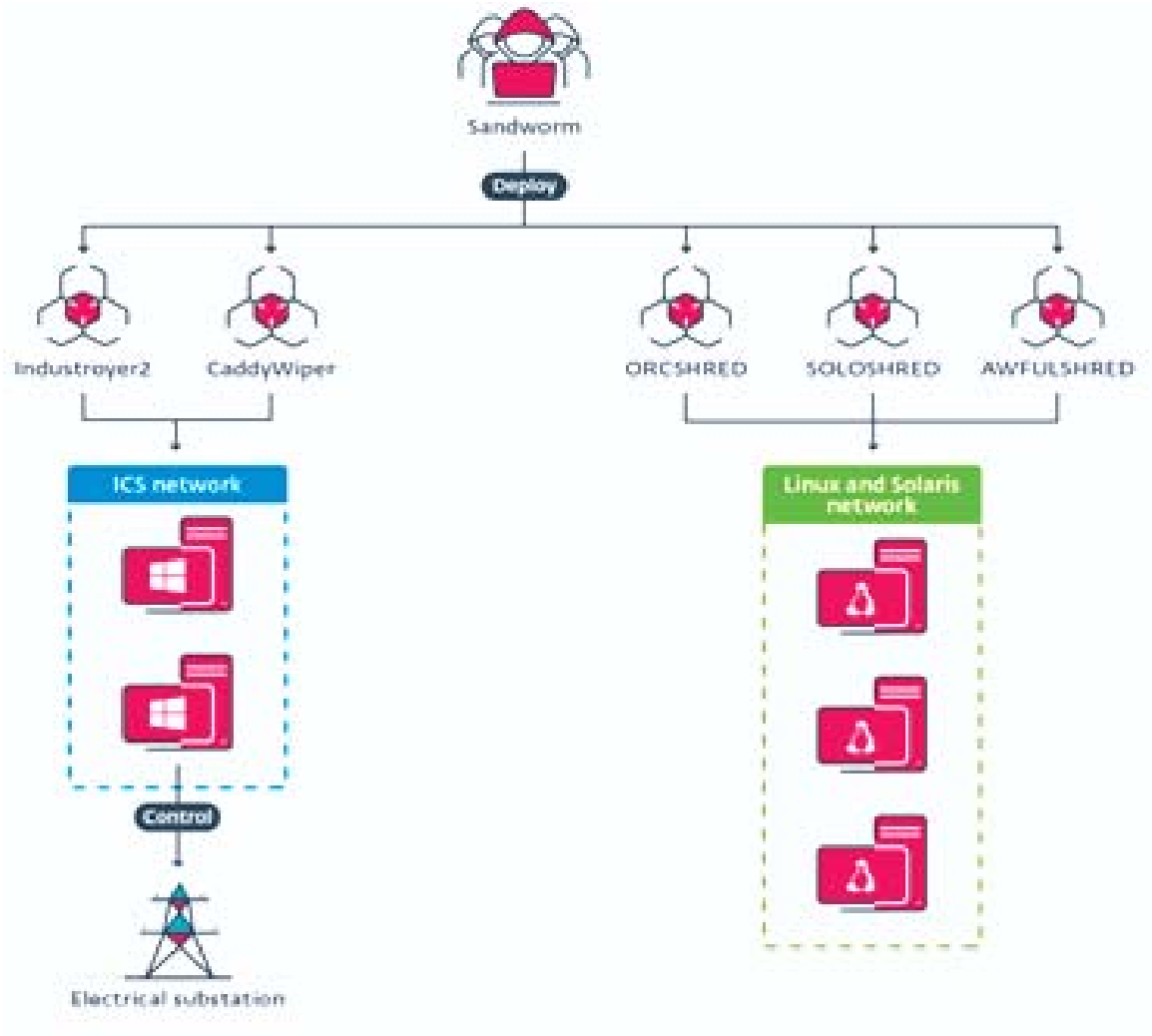


Рис. 8. Шкідливе програмне забезпечення, застосоване під час атаки на українську систему управління промисловістю (ICS) (дослідження компанії ESET)

Джерело: [5]

За даними фахівців компанії **ESET** [5], 8 квітня 2022 року о 14:58 зловмисниками було завантажено руйнівне шкідливе програм-

DOI: 10.34132/pard2022.15.02

не забезпечення **CaddyWiper** на пристроях Windows, Linux і Solaris у постачальника енергії. Того ж дня о 15:02 злочинна кібергрупа Sandworm створила заплановану задачу для запуску **Industroyer2**. О 16.10 зловмисниками був запланований запуск Industroyer2 для відключення електроенергії в Україні, а о 16:20 у той же день мав запуститись CaddyWiper на тому ж пристрої для видалення слідів Industroyer2. Варто нагадати, що подібні приклади кібернападів було зафіксовано у період з грудня 2015 року по грудень 2016 року в Україні. Зокрема, зловмисниками були здійснені руйнівні кібератаки на уряд та критичну інфраструктуру: на електричну мережу України, Міністерство фінансів та Державну казначейську службу, з використанням шкідливих програм, відомих як **BlackEnergy**, **Industroyer** та **KillDisk** [8, С. 497-501].

У 2020 році урядом США (обвинувальний акт) було звинувачено в участі в кібератаках, з використанням Industroyer і NotPetya, шість офіцерів російської військової частини 74455 Головного розвідувального управління (ГРУ) [9]. На думку фахівців компанії Microsoft, кібернапад на систему управління промисловістю (ICS) співпав з ескалацією військового впливу РФ на критичну інфраструктуру України на початку квітня. З огляду на реалізовані дії кібергруп РФ, які відображають і доповнюють військові дії, буде й надалі спостерігатись поступове збільшення кількості об'єктів для деструктивних кібератак, відповідно це буде відбуватись у прямій залежності від військових дій.

Разом з енергетичним сектором, майбутніх деструктивних атак може зазнати й сектор зв'язку в Україні, внаслідок його компрометації вже відомими й підозрюваними кібергрупами. Microsoft спостерігала як IRIDIUM, STRONTIUM та невідомі, але підозрювані у керуванні ними з боку РФ, зловмисники здійснювали компрометацію або розширювали наявний доступ до сектору комунікацій у квітні. Їхньою метою була IT-інфраструктура, яка підтримує цей сектор і головний Інтернет-провайдер**.**

Отже, оскільки війна триває, а країни світу надають військову допомогу Україні, або вживають санкції проти РФ, можна припустити, що зловмисники, керовані РФ, можуть здійснити кібератаки

у відповідь й за межі України. Про ці загрози корпорація Майкрософт повідомила своїх клієнтів та надала інформацію, яка може допомогти у ідентифікації та пом'якшенні загроз у мережах. Наразі Microsoft спостерігає, що зловмисники DEV-0586 та IRIDIUM діють стримано у виконанні деструктивних атак, обмежуючи розгортання шкідливих програм на конкретних цільових мережах. Однак, керовані РФ зловмисники активно намагаються отримати початковий доступ до уряду та організацій критичної інфраструктури по всьому світу, роблячи можливими майбутні атаки. Microsoft заохочує всі організації, які прямо чи опосередковано функціонують зараз в Україні, для захисту від загроз, активно стежити за подібними діями у своєму оточенні та запобігати їм.

Компанія Microsoft наразі здійснює постійну тісну координацію з українським урядом, а також з Європейським Союзом, європейськими державами, урядом США, НАТО та Організацією Об'єднаних Націй. Одним з головних глобальних зобов'язань компанії проголошено допомогу в захисті урядів і країн від кібератак [3]. 24 травня 2022 року відбулася зустріч віцепрем'єр-міністра-міністра цифрової трансформації України М. Федорова з президентом компанії Microsoft Б. Смітом.

Під час зустрічі М. Федоров зазначив, що «Україна продовжує плідну співпрацю з Microsoft та вдячна за підтримку, отриману від компанії під час війни з Росією. Команда Microsoft розглядає нові можливості стати «куратором» цифрової індустрії в часи відбудови України» [11].

Також Microsoft надав Україні безкоштовні хмарні сервіси до кінця 2022 року. Компанія виділила понад 242 мільйони доларів на підтримку України, зокрема 90 мільйонів доларів на гуманітарну допомогу, а також призупинила всі нові продажі продуктів і послуг у РФ. Наразі, в умовах війни, команда Microsoft сприяє документуванню воєнних злочинів РФ в Україні, й співпрацює з ООН щодо обміну інформацією про збитки від війни в Україні. Президент компанії Б. Сміт зазначив, що «Microsoft підтримував і буде підтримувати Україну далі. Це стосується як клієнтів продуктів та сервісів Microsoft, так і державних агенцій» [11].

DOI: 10.34132/pard2022.15.02

Таким чином, Україна співпрацює з багатьма представниками світової спільноти на рівні урядів, міжнародних об'єднань, з громадськими організаціями, технологічними корпораціями, фондами не лише щодо гуманітарної допомоги під час війни, а й у безпековій, військовій сферах. Зокрема, це стосується й співпраці СБУ та НАТО у сфері кібербезпеки. 5 квітня 2022 року відбулася взаємна інтеграція систем моніторингу загроз [12]. Служба безпеки України приєдналася до платформи НАТО з обміну інформацією про кіберзагрози - Multinational Malware Information Sharing Platform (MN MISP). Ситуаційний центр забезпечення кібербезпеки СБУ створив аналог цієї платформи в Україні у 2018 році - національну платформу **Malware Information Sharing Platform «Ukrainian Advantage»** (MISP-UA) (https://misp.gov.ua) для ефективної протидії кіберзагрозам і обміну даними щодо ризиків. «До платформи входять майже 1300 представників об'єктів критичної інфраструктури, урядових та військових ресурсів. В умовах гібридної агресії РФ, користувачі MISP-UA щоденно отримують індикатори кіберзагроз, встановлені за результатами розслідувань СБУ, а також мають можливість поділитись із закритою спільнотою власними даними» [12].

30 травня 2022 року українська делегація ДССЗЗІ вперше взяла участь у засіданні Керівного комітету Об'єднаного центру передових технологій з кібероборони НАТО (**CCDCOE**), під час якого було зазначено, що «приєднання України до CCDCOE – сприятиме посиленню міжнародної взаємодії у сфері кібербезпеки та кібероборони» [13]. Україна подала заявку на приєднання до CCDCOE ще в серпні 2021 року, а 4 березня 2022 заявку одностайно підтримали всі члени Керівного комітету. Наразі триває підготовка технічної угоди про вступ України до CCDCOE.

З початку повномасштабного вторгнення РФ в Україну **Google.org** і співробітники Google зробили мільйонні пожертвування та надали гранти державі на суму 45 млн доларів. Крім того, компанія однією з перших застосували санкції проти Росії. 25 травня 2022 року М. Федоров коментуючи співпрацю з Google, підкреслив, що «важливим кроком також було приєднання до санкцій. Призупинення реклами Google в Росії, співпраці з російськими рекламодавцями.

А також відмова в нових реєстраціях у хмарних сервісах, GooglePay та функції монетизації для YouTube в Росії. Крім того, з перших днів Google блокував рекламу та намагався забезпечити висвітлення війни найбільш коректним чином. З початку війни YouTube видалив понад 9000 каналів і 70 000 відео, які спотворювали правду про російську агресію» [14]. 26 лютого 2022 року Google на невизначений термін призупинив монетизацію російських державних ЗМІ у всьому світі, зокрема RT та Sputnik, а потім 2 березня YouTube заблокував усі канали, пов'язані з російськими державними ЗМІ у Європі. «Google також розширила кіберзахист для облікових записів українців. Дуже важливим для наших державних ресурсів та ЗМІ став Project Shield - Україна вдячна за безоплатний необмежений захист від DDoS-атак», - зазначив М. Федоров [14].

21 червня 2022 року Д. Коен, голова компанії Jigsaw, яка входить до складу Google, виступив з промовою на засіданні Ради Безпеки ООН, присвяченому Україні. Він зауважив, що коли Рада Безпеки була створена, ніхто не міг уявити, що майже 65% населення світу буде пов'язано таким складним утворенням як сучасний Інтернет. «Для війни в Україні на YouTube, TikTok та інших платформах завантажено більше годин відеоматеріалу, ніж хвилин конфлікту. Раніше в дискурсі були відсутні такі терміни, як «DDoS-атака», «шкідливе програмне забезпечення» (malware), «вірус», «тролінг», «переслідування в Інтернеті» (online harassment), «doxing» (збір та публікація особистої інформації про певну особу чи організацію), «DNS poisoning» (пошкодження цілісності даних) та «злом» (hacking). Ці поняття є новими для Ради Безпеки, але мотиви, які стоять за ними та наслідки - знайомі так само, як війни та конфлікти Інтернет став критичним сектором, який потрібно захопити під час війни» [7].

Д. Коен підкреслив, що «за секунди вміст здатний поширитись серед мільярдів людей, і пом'якшити можливу загрозу або навіть знищити демократичні системи. Це вивело цифрову та інформаційну війну на передній план геополітичних конфліктів» [7]. Він також зазначив, що Україна з 2014 року перетворилась на мішень для кібератак, і є відзеркаленням того, що чекає на весь світ під час

DOI: 10.34132/pard2022.15.02

ведення конфліктів у цифровому просторі. «Розподілені атаки типу «відмова в обслуговуванні» або «DDoS» є найбільш поширеними формами атаки. В Україні РФ розгорнула DDoS-атаки, які призвели до зниження з'єднання на 15-20 відсотків, а також у багатьох випадках Інтернет-з'єднання впало до нуля» [7]. Ці дії РФ пояснюються тим, що відключення інтернету та зв'язку на окупованих територіях та приєднання їх до російського інтернету є спробою РФ нав'язати уявлення у своїй правоті. Д. Коен закликав Раду Безпеки ООН до термінового розгляду цифрових наслідків війни та розробки законодавчих змін для запобігання цим загрозам. «У нас немає стримування в кібер-сфері і населення світу потрапило під перехресний вогонь. Держави повинні розробити доктрину стримування для кібер-сфери. Компанії та технологічні експерти мають необхідний досвід, але не існує магічного алгоритму чи єдиного рішення. Для захисту цифрового світу знадобляться численні експериментальні зусилля» [7].

Подолати проблему з відключенням інтернет-зв'язку в Україні під час війни допомогла компанія І. Маска – «**SpaceX**», надавши Україні доступ до широкосмугового інтернету, завдяки «**Starlink**». Starlink – це проєкт американської компанії SpaceX щодо розробки високопродуктивної супутникової платформи для виготовлення супутників зв'язку та запуску їх у космос, що забезпечує доступ до широкосмугового інтернету в будь-якій точці планети. 26 лютого 2022 року, у відповідь на прохання українського уряду, SpaceX як гуманітарну допомогу відправила тисячі супутникових тарілок Starlink до зони бойових дій. Протягом місяця кількість українських завантажень програми Starlink, яка використовується для підключення комп'ютерів і телефонів до супутникових тарілок, а отже, до сигналів супутникового Інтернету зросла з нуля до 215 000 (що становить 58% від їхньої загальної кількості у світі) (Див. рис. 9) [10].

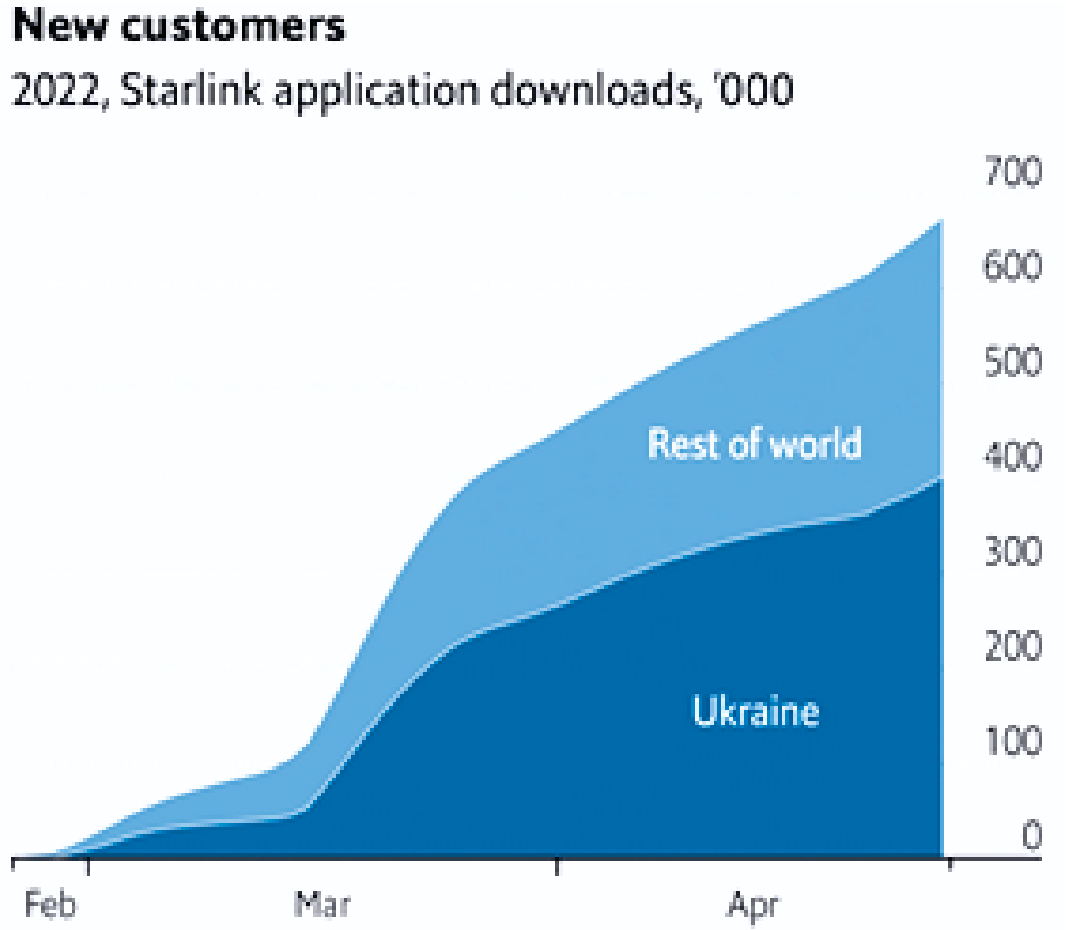


Рис. 9. Завантаження програми Starlink у 2022 році в Україні та світі

Джерело: [10]

З початку війни підключення до Інтернету було нестабільним. Російські війська завдали ударів по телевежах у Києві та Харкові. 21 березня Маріуполь втратив зв'язок після того, як війська РФ бомбардували офіси найбільшого в Україні інтернет-провайдера «Київстар», останнього, хто надавав послуги в оточеному місті. «Супутникові тарілки Starlink забезпечують життєдіяльність країни там, де немає іншого зв'язку. Значну кількість пристроїв привезли самостійно різні компанії, організації, громадські об'єднання і громадяни. Starlink надає можливість залишатися на зв'язку там, де немає альтернативи – стаціонарний та мобільний інтернет не працює через пошкодження, в тому числі й унаслідок воєнних дій, чи відключення енергопостачання, або ж у відповідному місці взагалі

DOI: 10.34132/pard2022.15.02

немає покриття» [15]. 19 квітня 2022 року віцепрем'єр-міністр – міністр цифрової трансформації М. Федоров, зазначив, що «понад 10 тис. станцій Starlink допомагають ЗСУ бути на зв'язку та реалізовувати спеціальні операції, підтримують роботу критичних енергетичних і телекомунікаційних об'єктів, закладів охорони здоров'я і навіть посівну кампанію, а також повертають до життя деокуповані території» [16]. В Україні зареєстрували представництво Starlink під назвою «StarlinkUkraine». Поки в країні немає власної наземної станції Starlink, але її планують побудувати після закінчення війни.

Американське видання **The Economist** у квітні 2022 року зазначило, що в Україні Starlink використовується військовими та лікарнями, але його сигнал слабкий на передовій. Нижче наведено особливості супутникового інтернету в Україні станом на 20 квітня 2022 року (Див. рис. 10) [10].

Рис. 10. Супутниковий інтернет-зв'язок Starlink в Україні
Джерело: [10]

«За даними data-компанії **Apptopia**, Starlink має приблизно 150 000 активних щоденних користувачів в Україні. Daily Telegraph повідомляє, що українські війська використовують Starlink для збору

розвідувальних даних і відстеження цілей для ударів безпілотників. Міністр охорони здоров'я України В. Ляшко зазначив, що лікарні уникають відключень електроенергії, використовуючи його сигнали. Проте зв'язок найслабший на сході України, осередку російської атаки, оскільки там орбітальні супутники знаходяться далі від своїх наземних станцій. 21 квітня SpaceX вивела на орбіту ще 53 супутники» [10].

Також Україні надає фінансову допомогу Швейцарія через Швейцарську агенцію розвитку та співробітництва (SDC). Це стосується Швейцарсько-української Програми «Електронне урядування для підзвітності влади та участі громади» (EGAP), яка реалізується у 2015-2023 роках Фондом Східна Європа та Фондом Innovabridge у партнерстві з Міністерством цифрової трансформації України. Згідно Програми втілюються два ключові компоненти: розвиток електронних послуг та електронної демократії на національному рівні, і в регіонах України (або на рівні громад). Зокрема, М. Федоров наголосив, що «фінансова допомога EGAP до та під час війни допомогла запровадити низку революційних та корисних соціальних послуг… Навіть під час війни, Міністерство цифрової трансформації продовжує спрощувати отримання послуг, запускати нові зручні сервіси та адаптувати вже наявні. Наша цифрова база та ваша фінансова підтримка допомогли швидко адаптуватися та бути ефективними у війні» [17]. У 2022 році заплановано розширення бюджету програми EGAP на 1,5 млн франків для підтримка проєктів цифрового відновлення України. «Програма EGAP допомогла в створенні порталу та застосунку Дія, порталу Дія.Цифрова освіта, розробці Платформи цифрової трансформації регіонів України Дія. Цифрова громада, та профінансувала запуск десятків сервісів Мінцифри, серед яких послуги для автоматичної реєстрації бізнесу, сервісу єМалятко, податкові послуги, електронна реєстрація місця проживання, місцеві петиції, електронні медичні висновки та ін.» [17].

Варто зазначити, що «через повномасштабну війну 13 ЦНАПів Київської, Чернігівської, Житомирської та Сумської областей залишилися зі зруйнованими приміщеннями та без техніки. Шведсь-

DOI: 10.34132/pard2022.15.02

ко-український Проєкт PROSTO «Підтримка доступності послуг в Україні» закупить та передасть громадам найнеобхідніші набори техніки для ЦНАПів на суму 780 000 гривень за зверненням Мінцифри» [18].

19 травня 2022 року під час зустрічі з головою Групи підтримки України в Єврокомісії К. Матерновою щодо приєднання України до програми «Цифрова Європа» М. Федоров подякував за підтримку та зазначив, що «ми вдячні Єврокомісії за оперативність та розпочаті консультації щодо приєднання України до участі в програмі «Цифрова Європа». Дуже розраховуємо на її підписання в липні цього року. Це допоможе Україні якнайшвидше імплементувати всі наші зобов'язання в цифровій сфері згідно з Угодою про асоціацію» [19].

Україна та ЄС також активно співпрацюють над реалізацією спільного плану у сфері електронних довірчих послуг, для їх взаємного визнання, що дозволить бізнесу отримувати онлайн-послуги за межами України. Про це 20 травня зазначив М. Федоров під час зустрічі з Генеральним директором Генерального директорату Європейської комісії з комунікаційних мереж, контенту та технологій (DG CONNECT) Р. Віолою. «Однак, поки така угода не укладена, потрібні альтернативні рішення для спрощення взаємин українського бізнесу з європейським. Наприклад, створення технічної можливості перевірки українських цифрових підписів у ЄС» [20].

15 червня 2022 року М. Федоров зустрівся з послом США в Україні Б. Брінк у кіберцентрі UA30 (CERT-UA). М. Федоров під час зустрічі зазначив, що «США - надійний партнер Мінцифри як з боку уряду, так і в контексті підтримки корпоративних санкцій найбільшими технологічними компаніями. Усі досягнення цієї двосторонньої співпраці стали фундаментом цифрового протистояння України в умовах повномасштабної війни». Зокрема, триває співпраця уряду з Агентством США з міжнародного розвитку, незалежним агентством федерального уряду США – USAID, для надання невійськової допомоги. USAID надає допомогу Мінцифрі та Держспецзв'язку у сфері кіберзахисту під час повномасштабної війни.

За сприяння USAID Україна отримала 5 тисяч станцій Starlink. Надзвичайний і Повноважний Посол США в Україні Б. Брінк підкреслила, що США продовжуватимуть надавати необхідну підтримку та сприяти розвитку цифровізації та кіберзахисту України. Зокрема, вона заявила, що «оскільки Міністерство цифрової трансформації прискорює рух України в майбутнє та захищає країну від наполегливих російських кібератак, США за допомогою механізмів USAID продовжуватимуть підтримувати міністра Федорова та його команду у важливій роботі із захисту України, її народу та їхнього демократичного майбутнього»[21].

Висновки. Отже, в результаті проведеного аналізу особливостей, стратегії, методів та масштабів нападу кіберсуб'єктів, керованих РФ, на цифрову інфраструктуру України, державні установи, стратегічні об'єкти критичної інфраструктури, організації третього сектору, встановлено, що ці дії є частиною масштабної «гібридної» війни проти України. Реалізація кібернападів РФ супроводжувалась й військовим нападом на заздалегідь скоординовані нею цілі.

Результати дослідження також доводять, що зловмисники використовували шкідливе програмне забезпечення в українських мережах напередодні вторгнення в Україну 24 лютого 2022 року. У січні 2022 року, Центр розвідки загроз Microsoft (MSTIC) виявив шкідливе програмне забезпечення у більш ніж десятках мереж України. За день до військового вторгнення оператори пов'язані з ГРУ, російською військовою розвідкою здійснили деструктивні атаки на сотні систем українського уряду, ІТ сектору, енергетичних та фінансових організацій. Діяльність, яку спостерігала компанія Microsoft, включала в себе спроби зловмисників знищити, порушити або потрапити в мережі державних установ, та об'єкти критичної інфраструктури, на деякі з них російські збройні сили одночасно здійснили наземні атаки та ракетні удари. Під час здійснення кібератак на цифрову інфраструктуру України зловмисники, керовані спецслужбами РФ, мали на меті знищення, або потрапляння у мережі державних установ та об'єкти критичної інфраструктури, для погіршення їх функціонування, для перешкоджання доступу громадян до надійної інформації та життєво важливих послуг.

DOI: 10.34132/pard2022.15.02

Кіберзлочинці використовують різноманітні методи отримання початкового доступу до своїх цілей, реалізуючи фішингові кампанії, використовуючи невиправлені вразливості локальних серверів Exchange і компрометацію постачальників IT-послуг. Цей початковий доступ дозволяє їм проводити операції зі знищення, вилучення даних, а також для довготривалого шпигунства та спостереження. Зловмисники часто змінюють своє шкідливе програмне забезпечення під час кожного застосування, щоб уникнути виявлення. Встановлено, що відомі і підозрювані російські кібергрупи, зокрема, STRONTIUM, IRIDIUM, DEV-0586, NOBELIUM, ACTINIUM, BROMINE, KRYPTON, працюють над компрометацією державних та недержавних установ в усіх регіонах України, а використання РФ кібератак, переважно пов'язане з її військовими операціями, спрямованими на служби та установи, які є важливими для цивільного населення. Деструктивні атаки є компонентом російських кібероперацій під час війни. Кібератаки тривають і загрожують життю та добробуту цивільного населення.

За прогнозами фахівців Microsoft, триваючі руйнівні кібератаки в Україні можуть бути ще більш тяжкими за наслідками, в тому числі нести загрози й для глобальної кібербезпеки. Зберігається небезпека використання злочинними кібергрупами таких можливостей для нападу як zero-days, атаки на критичну інфраструктуру, атаки на ланцюги постачання та інші нові методи в середньостроковій перспективі. Велика безпекова спільнота, прагне й надалі виявляти і пом'якшувати раніше невідомі вразливості та ланцюги атак, змушуючи диверсифіковану екосистему, з добре забезпеченими кіберсуб'єктами, закривати вразливості. Організації у всьому світі повинні визнати і підготуватися до реальності, де такі дії будуть відбуватися і навряд чи будуть обмежені певним доменом. Безпекові команди Microsoft, Google, Eset, Fortinet та інших компаній, а також уряди країн світу, тісно співпрацюють з українськими посадовими особами з кібербезпеки та співробітниками цих структур, організаціями та приватними підприємствами для виявлення і усунення загроз українським мережам. Microsoft встановив безпечні лінії зв'язку з ключовими посадовцями з кібербезпеки в Україні, щоб

допомогти українським державним установам, підприємствам та організаціям захиститися від атак. Це включало цілодобовий обмін даними про загрози та розгортання технічних контрзаходів для протидії шкідливому програмному забезпеченню.

Варто підкреслити, що оскільки війна в Україні триває, а країни світу надають військову допомогу Україні, або вживають санкції проти РФ, ймовірно, що зловмисники, керовані РФ, можуть здійснювати кібератаки у відповідь й за межами України. Керовані РФ зловмисники, активно намагаються отримати початковий доступ до уряду та організацій критичної інфраструктури по всьому світу, роблячи можливими майбутні атаки. Наразі в Україні триває процес розробки і розвитку власної моделі кіберзахисту держави в умовах протидії російській агресії, з використанням сучасних світових практик, практик країн НАТО та ЄС в означеній сфері. Розробка нових сучасних заходів боротьби з кібернападами українських фахівців та досвід цієї боротьби є нагальним для світової спільноти, оскільки використання кібератак є потужною стратегією дестабілізації та геополітичного впливу країн-агресорів.

Стаття надійшла до редакції: 06.03.22

CYBER WAR IN UKRAINE AND NATIONAL SECURITY CHALLENGES: CYBER ATTACKS ON DIGITAL INFRASTRUCTURE (GOVERNMENT AGENCIES, CRITICAL INFRASTRUCTURE, AND THIRD SECTOR ORGANIZATIONS)

Hanna Bondar, PhD in Political Sciences, Associate Professor at the Institute of Public Administration, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine.

The article is devoted to the analysis of the peculiarities of Russia's attacks on Ukraine in cyberspace synchronized with the beginning of a full-scale military invasion of the country on February 24, 2022. Challenges

DOI: 10.34132/pard2022.15.02

(threats) to the national security of Ukraine in cyberspace are analyzed. The peculiarities of cyber attacks on the digital infrastructure of Ukraine by criminals led by Russian special services to destroy, disrupt or enter the network of government agencies and critical infrastructure, to impair their functioning and to prevent access to reliable information and vital services. It is established that well-known and suspected Russian cyber groups are working to compromise government and non-government agencies in all regions of Ukraine, and the use of cyber attacks by Russia is mainly related to its military operations aimed at services and institutions important to civilians. The results of the study show that the attackers used malicious software on Ukrainian networks on the eve of the invasion of Ukraine on February 24, 2022. Ongoing destructive cyberattacks in Ukraine could be even more severe, including threats to global cybersecurity. Russian-led attackers are actively seeking initial access to government and critical infrastructure organizations worldwide, making future attacks possible. The peculiarities of close cooperation of governments, international associations, technology campaigns, foundations with Ukrainian officials responsible for cybersecurity and employees of these structures, organizations and private enterprises to identify and eliminate threats to Ukrainian networks are highlighted. It is established that cyberattacks aimed at Ukraine, including critical infrastructure (government, military, energy, industrial sector, mobile and Internet communications, media, etc.), can affect other countries, so it is emphasized the importance of close international cooperation in preventing, deterring and responding to attacks in cyberspace.

Key words: *cyberwar, cyber attacks, digital infrastructure, critical infrastructure, cybersecurity.*

Received: 06.03.22

References:

1. Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Digital Security Unit. April 27, 2022. (n.d.). *https://query.prod.cms.rt.microsoft.com.* Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

2. Burt, T. The hybrid war in Ukraine. April 27, 2022. *blogs.microsoft.com.* Retrieved from https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.

3. Smith, B. Digital technology and the war in Ukraine. February 28, 2022. *blogs.microsoft.com.* Retrieved from https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/.

4. Revay, G. An Overview of the Increasing Wiper Malware Threat. Threat Research. FortiGuard Labs. April 28, 2022. *https://www.fortinet.com.* Retrieved from https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

5. Industroer2: Industroyer reloaded. This ICS-capable malware targets a Ukrainian energy company. ESET Research.Welivesecurity by ESET. April 12, 2022. *www.welivesecurity.com.* Retrieved from https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

6. Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. Council of the EU. Press release. May 10, 2022. (n.d.). *https://www.consilium.europa.eu*. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

7. Cohen, J. Warning incitement of racial, religious hatred can trigger atrocity crimes, Special Adviser stresses states' legal obligation to prevent genocide. Russian Federation's Disinformation Campaign Aimed to Justify Invasion of Ukraine, Several Speakers Stress. Security Council. June 21, 2022. *https://reliefweb.int.* Retrieved from https://reliefweb.int/report/ukraine/warning-incitement-racial-religious-hatred-can-trigger-atrocity-crimes-special-adviser-stresses-states-legal-obligation-prevent-genocide

8. Yemelyanov, V., & Bondar, H. (2019). Kiberbezpeka yak skladova natsional′noyi bezpeky ta kiberzakhyst krytychnoyi infrastruktury Ukrayiny

DOI: 10.34132/pard2022.15.02

[Cybersecurity as a component of national security and cyber protection of critical infrastructure of Ukraine]. 10.09.2019. *Public Administration and Regional Development*, (5), 493-523. https://doi.org/10.34132/pard2019.05.02.

9. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. Department of Justice. Office of Public Affairs. An official website of the United States government. October 19, 2020. (n.d.). *https://www.justice.gov.* Retrieved from https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

10. Satellite internet is a hot new commodity in Ukraine. Starlink is being used by the military and hospitals, but its signal is weakest on the front line. The Economist. April 29, 2022 (Updated May1, 2022). (n.d.). *https://www.economist.com*. Retrieved from https://www.economist.com/graphic-detail/2022/04/29/satellite-internet-is-a-hot-new-commodity-in-ukraine.

11. Mykhaylo Fedorov zustrivsya z prezydentom Microsoft Bredom Smitom. 24 travnya 2022 roku. [Mikhail Fedorov met with Microsoft President Brad Smith. May 24, 2022]. (n.d.). *thedigital.gov.ua.* Retrieved from https://thedigital.gov.ua/news/mikhaylo-fedorov-zustrivsya-z-prezidentom-microsoft-bredom-smitom.

12. SBU ta NATO posylyly spivpratsyu u sferi kiberbezpeky: vidbulasya vzayemna intehratsiya systemy monitorynhu zahroz. 5 kvitnya 2022 roku [SSU ta NATO posylyly spivpratsyu u sferi kiberbezpeky: vidbulasya vzayemna intehratsiya systemy monitorynhu zahroz. April 5, 2022]. (n.d.). *ssu.gov.ua.* Retrieved from http://ssu.gov.ua/novyny/sbu-ta-nato-posylyly-spivpratsiu-u-sferi-kiberbezpeky-vidbulasia-vzaiemna-intehratsiia-system-monitorynhu-zahroz.

13. Ukrayins′ka delehatsiya vpershe vzyala uchast′ u zasidanni Kerivnoho komitetu Ob″yednanoho tsentru peredovykh tekhnolohiy z kiberoborony NATO (CCDCOE). Derzhavna sluzhba spetsial′noho zv'yazku ta zakhystu informatsiyi Ukrayiny. 30 travnya 2022 roku. [Ukrainian delegation participated in a meeting of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) for the first time. State service of special communications and information protection of Ukraine. May 30, 2022]. (n.d.). *cip.gov.ua.* Retrieved from https://cip.gov.ua/ua/news/ukrayinska-delegaciya-vpershe-vzyala-uchast-u-zasidanni-kerivnogo-komitetu-ob-yednanogo-centru-peredovikh-tekhnologii-z-kiberoboroni-nato-ccdcoe.

14. Mykhaylo Fedorov vruchyv pershu «Vidznaku myru» kompaniyi Google. Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny. 25 travnya 2022 roku [Mykhaylo Fedorov vruchyv pershu «Vidznaku myru» kompaniyi Google. Ministry and Committee for Digital Transformation of Ukraine. May 25, 2022]. (n.d.). *thedigital.gov.ua*. Retrieved from https://thedigital.gov.ua/news/mikhaylo-fedorov-vruchiv-pershu-vidznaku-miru-kompanii-google.

15. Vse, shcho vy khotily znaty pro Starlink, i ne znaly, yak spytaty. Derzhavna sluzhba spetsial′noho zv'yazku ta zakhystu informatsiyi Ukrayiny. 25 kvitnya 2022 roku. [Everything you wanted to know about Starlink and didn't know how to ask. State service of special communications and information protection of Ukraine. April 25, 2022]. (n.d.). *cip.gov.ua.* Retrieved from https://cip.gov.ua/ua/news/vse-sho-vi-khotili-znati-pro-starlink-i-ne-znali-yak-spitati.

16. Tkachuk, B. V Ukrayini zareyestruvaly predstavnytstvo Starlink. 27 kvitnya 2022 roku. [A Starlink representative office has been registered in Ukraine. April 27, 2022]. *hromadske.ua*. Retrieved from https://hromadske.ua/posts/v-ukrayini-zareyestruvali-predstavnictvo-starlink.

17. Ukraine is grateful to Switzerland for its support during the war, says Mykhailo Fedorov. Ministry of Digital Transformation of Ukraine. Government portal. May 23, 2022. (n.d.). *www.kmu.gov.ua.* Retrieved from https://www.kmu.gov.ua/en/news/ukrayina-vdyachna-shvejcariyi-za-pidtrimku-pid-chas-vijni-mihajlo-fedorov.

18. U deokupovanykh hromadakh z″yavyt′sya dostup do derzhposluh. Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny. 26 travnya 2022 roku. [Access to public services will be available in deoccupied communities. Ministry and Committee for Digital Transformation of Ukraine. May 26, 2022]. (n.d.). *thedigital.gov.ua.* Retrieved from https://thedigital.gov.ua/news/u-deokupovanikh-gromadakh-zyavitsya-dostup-do-derzhposlug.

19. Mykhaylo Fedorov obhovoryv pryyednannya Ukrayiny do prohramy «Tsyfrova Yevropa» na zustrichi z holovoyu Hrupy pidtrymky Ukrayiny v Yevrokomisiyi. Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny. 19 travnya 2022 roku. [Mykhailo Fedorov discussed Ukraine's accession to the Digital Europe program at a meeting with the Chairman of the Support Group of Ukraine in the European Commission. Ministry and Committee for Digital Transformation of Ukraine. May 19, 2022]. (n.d.). *thedigital.gov.ua*. Retrieved

DOI: 10.34132/pard2022.15.02

from https://thedigital.gov.ua/news/mikhaylo-fedorov-obgovoriv-priednannya-ukraini-do-programi-tsifrova-evropa-na-zustrichi-z-golovoyu-grupi-pidtrimki-ukraini-v-evrokomisii.

20. Ukrayina spodivayet′sya vzyaty uchast′ u prohrami «Tsyfrova Yevropa» vzhe ts′oho lita - Mykhaylo Fedorov na zustrichi z Komisarom YES iz pytan′ vnutrishn′oho rynku. Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny. 20 travnya 2022 roku. [Ukraine hopes to take part in the Digital Europe program this summer - Mykhailo Fedorov at a meeting with the EU Commissioner for Internal Market. Ministry and Committee for Digital Transformation of Ukraine. May 20, 2022]. (n.d.). *thedigital.gov.ua*. Retrieved from https://thedigital.gov.ua/news/ukraina-spodivaetsya-vzyati-uchast-u-programi-tsifrova-evropa-vzhe-tsogo-lita-mikhaylo-fedorov-na-zustrichi-z-komisarom-es-iz-pitan-vnutrishnogo-rinku**.**

21. Mykhaylo Fedorov zustrivsya z poslom SSHA v Ukrayini Bridzhyt Brink**.** Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny. 15 chervnya 2022 roku. **[**Mikhail Fedorov met with US Ambassador to Ukraine Bridget Brink. Ministry and Committee for Digital Transformation of Ukraine. June 15, 2022**].** https://thedigital.gov.ua/news/mikhaylo-fedorov-zustrivsya-z-poslom-ssha-v-ukraini-bridzhit-brink

Відомості про автора / Information about the Author

Бондар Ганна Леонідівна: Чорноморський національний університет ім. Петра Могили: вул. 68 десантників 10, Миколаїв, 54003, Україна.

Hanna Bondar: Petro Mohyla Black Sea National University: 68 Desantnykiv str. 10, Mykolaiv, 54003, Ukraine.

ORCID.ORG/0000-0003-4112-263X

E-mail: gannabondar.ua@gmail.com