УДК 004.056
DOI: 10.31673/2409-7292.2022.010615

Веселков Н.Л., Вдовиченко М.С., Кукшин Д.В., Каленський Ю.М., Герніченко Г.Д.

ДОСЛІДЖЕННЯ УКРАЇНО-РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ ПРОТИДІЇ ПІД ЧАС ВІЙНИ НА ДОНБАСІ ТА ПОВНОМАШТАБНОГО ВТОРГНЕННЯ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ТЕРИТОРІЮ УКРАЇНИ

Розглянуто реалізація атак в кіберпросторі під час Україно-Російської війни, прикладки як інформаційно-дезінформаційних атак, так і кібератак на інфраструктуру українських компаній та уряду.

Ключові слова: кібервійна, дезінформація, кібератаки, Росія, Україна, війна, фейки.

Вступ

Українські фахівці з кібербезпеки постійно стикаюся з атаками з боку Росії в кіберпросторі. Це як і повноцінні кібератаки, які завдають мільйоні збитки, так і інформаційні атаки, які націлені на населення і цілю яких є поширення ідеологій та дезінформація населення. В цій статі ми розглянемо методи пропаганди та дезінформації Росії в період з 2014 по 2022 роки, а також кібератаки на українськи компанії та уряд за той самий період.

Інформаційна війна. Теорія

На сьогоднішній час інформаційна війна – це один із найпотужніших видів зброї. Вплив інформації на маси становить дуже велику силу, таким чином при вдалому маніпулюванні на людську свідомість можна досягти найрізноманітніших цілей: знешкодити свого опонента, позбавитись від конкурентів або навіть розпочати війну, як у випадку з Іраком.

Замість застарілих ідеологій ведення війн четвертого покоління (Друга Світова Війна, Велика Вітчизняна Війна) та п’ятого покоління (з застосуванням ядерної зброї) стають актуальними ідеології ведення війн шостого покоління, які можна описати наступними основними постулатами:

перемога у війні зовсім не в тому, щоб захопити території опонента;

ядерна зброя не є найпотужнішим методом ведення війни;

заподіяння опоненту непоправної шкоди методом застосування високоточної зброї, щоб вивести з ладу найважливіші об’єкти або засоби комунікацій (інфраструктури управління) – цього цілком достатньо для досягнення цілей війни;

вважаються недоречними масові жертви серед мирного населення або заподіяння екологічної або економічної шкоди;

Метою інформаційної війни являється посилення власних моральних та матеріальних сил, та послаблення їх у стані конкурента або опонента.

Інформаційна війна є складовою ідеологічної боротьби. До наслідків таких війн не входять безпосередньо людські жертви, руйнування або позбавлення ресурсів для проживання, таких як їжа та житло. Саме через це інформаційні війни породжують небезпечну безпечність у відношенні до них. Тому не зважаючи на це, руйнування, які викликають інформаційні війни у психології суспільства та особистості цілком співмірні за масштабом і значенням, а іноді й перевищують наслідки збройних війн.

Причиною такого здебільшого безтурботного ставлення є те, що не всі розуміють, що саме таке “Інформаційна війна”.

Інформаційна війна. Період АТО/ООС (2014-2021 роки)

В умовах бойових дій на Сході України, а також окупації Криму результат інформаційно-психологічного впливу російських ЗМІ на українську спільноту виявився в спотворенні подій, об'єднаних з АТО, недоброзичливе ставлення людей з орієнтальних ареалів західної частини держави, поширенні дезінформації, а також зухвалому народному поділу населення. Регулярно обговорюється мовне питання, проводяться суперечки навколо багатоетнічності України, виникають заборони на ряд вітчизняних кінофільмів і телеканалів,

відбувається хід декомунізації в усіх сферах колективного життя. Безперечно, все має свої плюси, проте і мінуси теж. Така відносна ізоляція від російських реалій ще не означає, що інформативна протидію з боку Росії в майбутньому не буде здійснюватися. Деякі люди в пошуках інформації звертаються до інтернет-ЗМІ, де немає ніяких заборон і який представляється неперевершеним і перспективним майданчиком світу ведення інформативною війни.

Проаналізувавши багато Інтернет-ЗМІ, які беруть участь у російській інформаційній війні, можна побачити, що їх діяльність базується на розповсюдженні неправдивої інформації, так званої "фейкової", метою якої є введення українського населення в оману. Проаналізувавши багато Інтернет-ЗМІ, які беруть участь у російській інформаційній війні, можна побачити, що їх діяльність базується на розповсюдженні неправдивої інформації, так званої "підробки", метою якої є введення України в оману та Росії. Населення Росії. Ця політика російського уряду спрямована на те, щоб викликати недовіру до українського уряду та суспільства, шукаючи найліпшу причину, щоб приховати країну, яка насправді перша вчинила агресію. На веб-сайтах Інтернет-видань, будь то Росія чи нещодавно створена Народно-Демократична Республіка та Республіка ЛНР, матеріали розміщуються під неперевіреними заголовками, що стосуються вигаданих "українських націоналістів" та "Націоналістичного табору"; територій на сході України, не підвідомчі ДНР вважаються окупованими. Під заголовком є образливі заяви на адресу українських військових та влади, часто розміщуються анонімні матеріали, а в описі вигаданого інциденту не згадуються джерела інформації. Серед інтернет-ЗМІ, які займається дезінформацією людей, вигадуючи матеріали, можна знайти: “Молот правды”, “Новости Донецкой Республики”, інформаційне агентство “Новороссия”, “Комсомольская правда”, “РИА-новости”, “V-news”. Ці портали розповсюджують в інтернеті інформацію неправдиву, фейкову, та яка не відповідає дійсності.

В Інтернеті можна знайти багато сайтів, які поширюють неправдиву інформацію про Україну та війну з Росією. За допомогою російського журналіста Дмитра Кисельова "ukraina.ru" було створено як інформаційний ресурс. Відразу стає ясно, що сайт є прямим джерелом упереджень та неправдивої інформації. Інтернет-видання використовують маніпулятивні заголовки, щоб повідомляти про дії бойовиків у Донецькій області. Новостворені сепаратистські Інтернет-ЗМІ мають на меті ввести в оману щодо діяльності українського уряду та армії, українського суспільства та мешканців окупованих територіях, щоб зменшити моральний дух та поширити страх, паніку та недовіру до тих, хто намагається захищати цілісність, незалежність та єдність України. Поширення фейкових новин та маніпулювання громадською думкою є основними інструментами впливу на людей.

Рис.1. Російська пропаганда, приклад №1

Російський веб-сайт Navigator оголосив, що зона озброєних конфліктів в Донецькій області розширюється, населення залишає свої домівки, а кількість поранених збільшується. На фотографіях, що додаються до новин, видно, як горить місто біля Путилівського мосту. Насправді пожежі та вибухи відбувалися за допомогою Photoshop.

У соціальній мережі “Вконтакте”, міністр оборони ДНР Ігор Стрєлков опублікував знімок палаючого бронетранспортеру. "У Донбасі почалася тотальна помста хунті! Як ми і обіцяли!"- саме так прокоментував цю фотографію міністр оборони. Проте насправді фото палаючого бронетранспортеру було зроблено в Китаї 3 червня 1989 на підступах до площі Тяньаньмень.

Рис. 2. Російська пропаганда, приклад №2

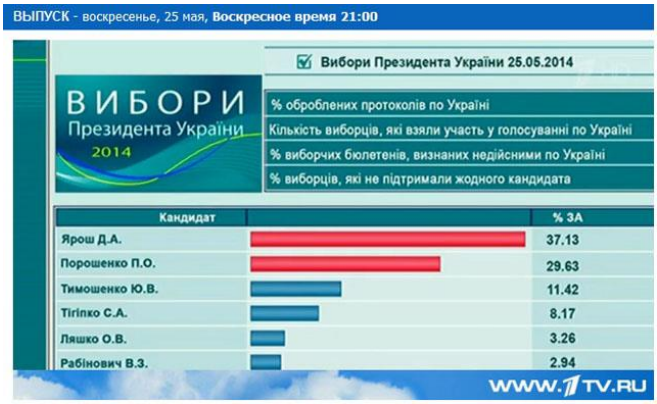

Рис. 3. Російська пропаганда, приклад №3

У недільному номері за 25 травня 2014 (день виборів президента України) російський "Перший канал" опублікував скріншот веб-сайту Центральної виборчої комісії, де показано, що лідер Правого сектора Дмитро Ярош отримав 37,13% голосів на виборах. У той же час, за даними Першого каналу, президентська кампанія за президента Петра Порошенка знаходиться лише на другому місці, що становить 29,63% голосів.

Новоросс.info опублікував новину про те, що «каратель» Коломойського (екс-губернатор Дніпропетровської області) побив ногами й кийками матерів солдатів із західної України, які перекрили дорогу та вимагали від нього, щоб їхні сини повернувся з каральної операції на південному сході. До новини було прикріплено кадр із відеозапису, який насправді було зроблено в Одесі в 2010 році, тоді перехожі побили водія, який збив жінку на тротуарі.

Рис. 4. Російська пропаганда, приклад №4

Інформаційна війна. Період вторгнення Росії на територію України 24 лютого 2022 року

Після початку повномасштабної війни 24 лютого 2022 року, Російська пропаганда почала створювати величезну кількість фейків стосовно ходу цієї війни. Машина пропаганди в Росії набрала шалених обертів, починаючи від постійних репортажів на росЗМІ про “вдале проведення спецоперації на Донбасі” до впровадження кримінального переслідування за

розповсюдження інформації пов’язаного з війною, яке розходитись з “офіційною” інформацією.

Населення України на фоні стресу почало сприймати дуже велику кількість інформації. В перші дні війни люди почали сприймати інформацію не тільки з звичних джерел, таких як, радіо, телебачення і незалежних ЗМІ, а й з різних новинних каналів в месенджерах та соціальних мережах. Такі різноманіття призвело до того, що люди почали отримувати дуже багато фейкової інформації.

Для аналізу фейків та дезінформації, ми провели аналіз заяв Центру протидії дезінформації при РНБО. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою. Робота Центру протидії дезінформації охоплює такі сфери як воєнний напрям, боротьбу зі злочинністю та корупцією, зовнішню та внутрішню політику, економіку, інфраструктуру, екологію, охорону здоров'я, соціальну сферу та науково-технологічний напрям. Але основна увага зосереджена на протидії поширенню неправдивої інформації в Інтернеті та фейків у медіа. Центр не має каральних функцій за дезінформацію і не зможе застосовувати санкції, але може вносити подання до РНБО щодо певних порушень.

Розглянемо деякі фейки, які знайшли аналітики центру.

На тимчасово захоплених територіях окупанти нині розгорнули цілу інформаційну операцію з поширення брехні, що ґрунтується на рекламі «добровільної» депортації на далекий схід. Так, по всіх чатах і групах, що є під контролем кремля, під виглядом волонтерів масово розповсюджують різні повідомлення «від друга» разом з гарними фото, що рекламують далекий схід.

На цю антилюдську акцію звернув увагу радник міського голови Маріуполя Петро Андрющенко.

Дедалі більше надходить інформації, що люди відмовляються їхати з Таганрога на далекий схід і масово тікають з точки посадки в потяг. Окупант розгорнув масовану інформатаку для запобігання подібному прояву незламності маріупольців, – написав Петро Андрющенко.

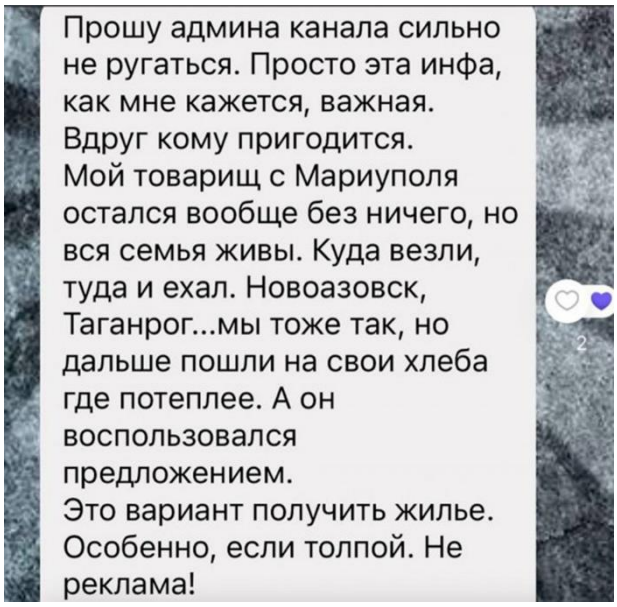

Рис. 5. Приклад дезінформації населення в тимчасово окупованому Маріуполі

Центр протидії дезінформації при РНБО України попереджає: російська пропаганда згенерувала та почала тиражувати фейк щодо того, що в Бучі українські військові використовували заборонені шрапнельні снаряди ЗШ-1.

Рис. 6. Попередження про фейк від ЦПД

Основним аргументом, до якого апелюють пропагандисти, є те, що «гаубиці Д-30, які й відстрілюють такий снаряд, у РФ застосовуються мало і переважно перебувають на консервації, а от українська армія такі гаубиці широко використовує». Однак цей аргумент не витримує жодної критики, оскільки:

ящики з російськими снарядами ЗШ-1 було виявлено в с. Андріївка Київської області;

перекидання гаубиць Д-30, які належать ЗС РФ, було зафіксовано (https://t.me/Hajun_BY/1988) 11 березня на території Білорусі;

перекидання САУ 2С1 «Гвоздика», які належать ЗС РФ, та також відстрілюють снаряд ЗШ-1, було зафіксовано (https://t.me/Hajun_BY/2590) 19 березня на території Білорусі.

Центр протидії дезінформації при РНБО України наводить найпопулярніші пропагандистські тези РФ, що намагаються посіяти паніку і недовіру до влади України:

дефіцит пального в країні;

нестача продовольства, голод;

крадіжки гуманітарної чи військової допомоги.

Саме такі тези просуває російська пропаганда і всі проросійські ЗМІ на території України.

Інформаційна війна. Кібератаки в українському кіберпросторі

Починаючи з 2014 року, Україна постійно була під прицілом російських спецслужб та хакерських угрупувань повязаних з ними. Розберемо деякі наймаштабніші кібератаки на український кіберпростір до 2022 року.

Petya.A

Petya.A – програма-вимагач, яка націлена на комп'ютери з операційної системи Windows.

Відповідно до аналізу Microsoft перші зараження відбулися Україні, де приблизно 12000 машин зіткнулися із загрозою. Потім зараження відбулося в інших 64 країнах, включаючи Бельгію, Бразилію, Німеччину, Росію та Сполучені Штати.

У цієї програми вимагача є можливості Worm, які дозволяли йому переміщатися мережею. Це зовсім новий різновид вимагачів, складніший.

Початкове зараження пов'язане із уразливістю програмного забезпечення для подання звітності MEDoc. Цей вектор довго обговорювався новинними ЗМІ та дослідниками в області інформаційної безпеки, в тому числі кібер-поліцією України, але цей факт не мав лише прямих підтверджень. Хоча незабаром компанія Microsoft знайшла докази того, що декілька активних заражень вимагачів спочатку були запущені в рамках легального процесу. Процес оновлення MEDoc і був процесом зараження.

Завдяки додатковим можливостям переміщенням нового вимагача, для зараження мережі потрібно всього одна заражена машина. Функціональність поширення програми-вимагача складається з декількох методів, що відповідають за:

крадіжку облікових даних або повторне використання реальних активних сеансів;

використання файлових ресурсів для передачі шкідливого файлу між комп'ютерами в одній мережі;

використання активних легальних функцій для виконання корисного навантаження або використання уразливостей SMB для не оновлених комп'ютерів.

Це шкідливе програмне забезпечення видаляє інструмент для вивантаження облікових даних (зазвичай у вигляді файлу .tmp в директорії %Temp%). Поставляється в 32-бітному та 64-бітному варіантах. Оскільки користувачі можуть входити в систему з використанням прав локального адміністратора і відкривають активні сеанси на декількох комп'ютерах, вкрадені облікові дані можуть забезпечити такий самий рівень доступу, який користувач має на інших комп'ютерах.

Отримавши дійсні облікові дані, програма-вимагач сканує мережу, щоб встановити з'єднання через tcp порти: 139 та 445. Для кожної підмережі він збирає всі клієнти (використовуючи DhcpEnumSubnetClients ()) для сканування служб. Якщо він отримує відповідь, шкідлива програма намагається розповсюдити двійковий файл на віддаленій машині, використовуючи звичайні функції з напередодні вкраденими обліковими даними. Потім за допомогою PSEXEC або WMIC намагається віддалено запустити програму-вимагач.

Програма-вимагач намагається видалити файл psexec.exe (dllhost.dat) та замінити на шкідливу програму. Потім сканує мережу на наявність загальних ресурсів адміністратора, розповсюджує себе мережею і виконує віддалене копіювання шкідливого двійкового файлу з використанням PSEXEC.

На додаток до скидання облікових даних, шкідлива програма намагається вкрасти облікові дані, використовуючи функцію CredEnumerateW, щоб отримати всі інші облікові дані, які можуть зберігатися в сховищі облікових даних.

Petya.A також може поширюватися за допомогою експлойта для уразливості протоколу EternalBlue. Крім того, цей вимагач також використовує другий експлойт EternalRomance. Ці уразливості були виправлені в оновленні безпеки MS17-010.

Поведінка шифрування цього вимагача залежить від рівня привілеїв і процесів, які будуть запущені на комп'ютері. Це досягається шляхом використання алгоритму хешування на основі XOR для імен процесів і перевірки наступних хеш-значень для виключення поведінки.

Industroyer (CRASHOVERRIDE)

Crashoverride є першим публічно відомим шкідливим ПЗ, призначеним для впливу на роботу електричних мереж. Незважаючи на те, що певну увагу вже були кібератаки на автоматизованої системи управління (АСУ), CRASHOVERRIDE, більш широкі масштаби атаки та передумови для її виконання були прикро недооцінені.

Crashoverride значною мірою покладався на досить стандартні методи вторгнення для досягнення своїх результатів. Розуміючи цю методологію і те, як ці методи можуть контролюватися і виявлятися, власники активів і можуть почати виявляти прогалини в області виявлення і видимості, з тим щоб використовувати такі методи в майбутньому. Хоча Crashoverride ефективно представляє собою нове додаток шкідливих програм для отримання фізичного впливу, основні методи для вторгнення і розгортання будуть помітними.

На момент свого відкриття Crashoverride був другим публічно відомим шкідливим програмним забезпеченням, націленим на АСУ, і першим, хто націлився на електричну мережу. У той час як попередні операції були прийняті місце проти роботи електромереж ніхто не використав шкідливе ПО для фактичного впливу.

Industroyer (Crashoverride) – це модульна шкідлива програмне забезпечення. Його основним компонентом є бекдор, який використовувався зловмисниками для управління атакою: він встановлює і контролює інші компоненти і підключається до віддаленого сервера для отримання команд і передачі звітів зловмисникам.

Відмінною рисою Industroyer від інших шкідливих ПЗ, націлених на інфраструктури, є використання чотирьох компонентів корисного навантаження, які призначені для прямого управління комутаторами та автоматичними вимикачами на розподільній підстанції. Кожен з цих компонентів призначений для конкретних протоколів зв'язку.

Як правило, корисні навантаження працюють поетапно, метою яких є відображення мережі, а потім пошук і видача команд, які будуть працювати з конкретними промисловими пристроями управління. Industroyer показує глибоке знання і розуміння авторами систем промислового контролю.

Industroyer містить ще кілька функцій, призначених для того, щоб дозволити йому залишатися не поміченим під радаром, забезпечити стійкість шкідливого ПЗ і знищити всі його сліди після того, як він виконає свою роботу. Наприклад, зв'язок з серверами C&C, прихований браузером Tor, може бути обмежений неробочими годинами. Крім того, він використовує додатковий бекдор, що маскується під додаток "Блокнот", призначений для відновлення доступу до цільової мережі в разі виявлення або відключення основного бекдора.

Модуль очищення призначений для стирання критично важливих для системи ключів реєстру та перезапису файлів, що робить систему не можливим завантаження системи і ускладнює відновлення.

Також інтерес для зловмисників мав сканер портів, який відображає мережу, намагаючись знайти відповідні комп'ютери. Зловмисники створили власний інструмент замість використання наявних програмних забезпечень.

Останній модуль – це інструмент проведення атаки "відмова в обслуговуванні", який використовує уразливість CVE-2015-5374 в пристроях Siprotec компанії Siemens і може зробити так, що цільові пристрої не будуть відповідати.

Industroyer можна використовувати для атаки на будь-яку промислову систему управління з використанням деяких цільових протоколів зв'язку, деякі компоненти в аналізованих зразках були призначені для роботи з конкретним обладнанням.

Завдяки своїй здатності зберігатися в системі і цінній інформації для налаштування корисних навантажень, зловмисники можуть адаптувати шкідливе ПЗ до будь-якого середовища, що робить його надзвичайно небезпечним.

Кібератаки перед та після вторгнення Росії на територію України

21 лютого 2022 року Державне агентство спеціального зв'язку та захисту інформації України повідомило, що CERT-UA може зламати домен .ua 22 лютого.

23 лютого 2022 року, за день до широкого вторгнення Росії в Україну, були зафіксовані кібератаки на державні ресурси та банки. Нова хвиля кібератак почалася близько 16:00 із знищення веб-сайтів Верховної Ради, Кабінету Міністрів України та Міністерства закордонних справ. Міністерство освіти і науки заблокувало доступ до свого сайту, щоб запобігти кібератакам. За словами міністра цифрової трансформації Федорова, портал і сайт

програми «Дія» успішно борються з атакою. Пізніше стало відомо, що скомпрометовані також сайти Служби безпеки України, стратегічних зон, Міністерства інфраструктури та агрополітики. Останній сайт має той самий інтерфейс, що й перша атака 14 січня.

Рис. 7. Дефейс повідомлення після атак

Згідно з дослідженням ESET, шкідливе програмне забезпечення HermeticWiper, назване на честь сертифіката підписання цифрового коду кіпрської компанії Hermetic Digital Ltd., почало працювати на зламаних веб-сайтах після DDoS-атаки 23 лютого. Метою цих шкідливих програм є знищення інформації в базі даних. Вірус було виявлено близько 17:00 23 лютого, але мітка часу вказує, що він був зібраний 28 грудня 2021 року.

Рис. 8. Хронологія вірусів класу Wiper

Експерти CERT-UA також розкрили серію атак, спланованих російським спецназом. Планом зловмисника є відключення кількох елементів інфраструктури цілі, а саме:

високовольтні підстанції – за допомогою шкідливої програми INDUSTROYER2; крім того, кожен виконуваний файл містить статично заданий набір унікальних параметрів для кожної підстанції (дата складання файлу: 23.03.2022);

електронні комп'ютери (комп'ютери) під керуванням операційної системи Windows (комп'ютери користувачів, сервери та АРМ АСУ ТП) – з використанням шкідливої програми для знищення програми CADDYWIPER; у цьому випадку розшифровка та запуск останньої передбачає використання ARGUEPATCH навантажувач і TAILJUMP Silkcode;

серверне обладнання під керуванням операційної системи Linux - з використанням шкідливих руйнівних скриптів ORCSHRED, SOLOSHRED, AWFULSHRED;

забезпечує можливість горизонтального переміщення між сегментами локальної мережі шляхом створення ланцюжка тунелів SSH. IMPACKET використовується для віддаленого виконання команд. Відомо, що організація-жертва зазнала двох хвиль атак. Закриття підстанції та виведення з експлуатації інфраструктури підприємства було заплановано на вечір п’ятниці, 8 квітня 2022 року. При цьому виконання шкідливих схем поки що заблоковано. Для виявлення ознак подібних загроз в інших українських організаціях обмеженій кількості міжнародних партнерів та українських енергетичних компаній було надано оперативну інформацію з TLP: рівень доступу AMBER, включаючи зразки шкідливих програм, індикатори компромісу та правила Yara.

Висновки

1. Росія постійно атакує Україну в кіберпросторі і розповсюджує дезінформацію.
2. Враховуючи надвисокий ступінь небезпеки, що несуть своєю діяльністю суб’єкти інформаційних війн усім державам (зокрема їх органам державної влади), державним структурам та міжнародним організаціям необхідно виробити відповідну нормативно-правову базу з урахуванням усіх можливостей сучасних інформаційно-телекомунікаційних технологій.
3. В сучасній Україні є відповідні органи і експерти, які в співпраці з міжнародними колегами можуть ефективно протидіяти кібератакам зі сторони Росії та різних хакерських груп.

Перелік посилань

1. Україна стала ціллю руйнівних атак до та під час російського вторгнення. [Електронний ресурс] – Режим доступу: https://eset.ua/ua/news/view/948/ukraina-stala-czelyu-razrushitelnykh-atak-do-i-vo-vremya-rossijskogo-vtorzheniya?_ga=2.143391734.257451860.1653291403-331853595.1631005752.
2. Ismail Erkan, Chris Evans The influence of eWOM in social media on consumers’ purchase intentions: An extended approach to information adoption // Computers in Human Behavior, 2016. Volume 61, Pages 47-55
3. Международное волонтерское сообщество InformNapalm [Електронний ресурс] – Режим доступу: https://informnapalm.org/
4. Пузняк З.М. Методика виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, Д.А. Шеремет // Сучасний захист інформації. 2017. - №3. – С.50-55
5. Рада національної безпеки і оборони України. [Електронний ресурс] – Режим доступу: https://www.rnbo.gov.ua/.
6. Кібератаки на українські державні сайти (2022). [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/ (2022).

Надійшла: 16.03.2022 Рецензент: к.т.н., доцент Дзюба Т.М.