УДК 342.951

БІЛАН І.А., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1237-1565.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СПЕЦСЛУЖБАМИ КРАЇНИ-АГРЕСОРА

DOI...

Анотація. *Визначено поняття та зміст шкідливого програмного забезпечення. Розкрито форми поширення шкідливого програмного забезпечення. Визначено загрози, які пов'язані із поширенням шкідливого програмного забезпечення. Деталізовано роль та місце спецслужб РФ щодо поширення шкідливого програмного забезпечення в контексті кібератак за участю хакерів та кіберзлочинців. Проведено маштабування цілей за результатами злочинної діяльності російських хакерів. Визначено об'єкти хакерських посягань на замовлення рф у світових вимірах. Наведено приклади зловмисних дій російських кіберзлочинців та результати їх наслідків для деяких країн ЄС та США. Окреслені сучасні ініціативи світової спільноти щодо системної та узгодженої боротьби з програмами-вимагачами за участю України. Зроблено прогноз щодо розвитку ситуації, подальших напрямків, акцентів діяльності хакерів та кіберзлочинців на замовлення російських спецслужб в умовах кібервійни.*

Ключові слова: *шкідливе програмне забезпечення, кібербезпека, кібератака, кібершпигунство, кіберпростір, спецслужба, національна безпека, хакерські атаки.*

Summary. *The concepts and characteristics of malware are defined. The forms of malware are highlighted. The threats associated with the spread of malicious software have been identified. The role and place of the special services of the russian federation regarding the spread of malicious software in the context of cyberattacks involving hackers and cybercriminals are detailed. The targets have been scaled based on the results of the criminal activity of russian hackers. The objects of hacking attacks ordered by the Kremlin in global dimensions have been identified. The examples of malicious actions of russian cybercriminals and the results of their consequences for some EU countries and the USA are given. The plan and the directions of its implementation by the aggressor state in the cyberspace of Ukraine are revealed. The modern initiatives of the world community regarding the systematic and coordinated fight against ransomware with the participation of Ukraine are outlined. A forecast regarding the further situation development, directions and emphasis of the activities of hackers and cybercriminals on behalf of the russian special services in the conditions of cyberwar was made.*

Keywords: *malware, cyber security, cyber attack, cyber espionage, cyber space, special service, national security, hacker attacks.*

Постановка проблеми. 24 лютого 2022 року держава-агресор вдарила ракетами не тільки по українських містах та об'єктах критичної інформаційної інфраструктури, але й вдалася до масових кібератак. Одночасно розпочалася перша у світі кібервійна, яка ніколи не закінчиться у кібер домені. Так, напередодні ввечері, 23 лютого 2023 року, експерти зафіксували у кіберпросторі роботу шкідливого програмного забезпечення під назвою "HermeticWiper", яке видаляє дані. Ця атака готувалася за декілька місяців шляхом аналізу вразливості діючих цифрових систем та закладання плагінів у них, а датою створення ШПЗ "HermeticWiper" спеціалісти вважають кінець 2021 року. 23 лютого 2023 року рф здійснила масштабну кібератаку на українські веб-ресурси. Проте ця атака не

призвела до значних збитків та порушень штатного функціонування інформаційно-комунікаційних систем та не вплинула на стабільний стан виконання державними органами своїх повноважень. Вже наступного дня разом із “HermeticWiper” активно використовувалася програма-вимагач “HermeticRansom” для відволікання уваги українських користувачів. А згодом з’явилася ще одна, яка знищує дані, – “IssacWiper”.

З цією метою держава-агресор залучає вмотивованих хакерів, зловмисників та досвідчених ІТ-спеціалістів. Найбільше “уваги” кіберзлочинці та хакери приділяють інформаційним порталам українського уряду та місцевих органів влади, структурам сектору безпеки та оборони. Найпоширенішими методами таких атак є перманентне збирання інформації OSINT, запуск шкідливого програмного коду та втручання або спроба втручання в ту чи іншу державну цифрову інформаційну інфраструктуру. Таким чином, завдяки постійному розширенню цифрової інфраструктури, зокрема, створенню нових додатків та сервісів, віддалених робочих місць та переходу в хмарне середовище, кількість потенційних кібератак ворога постійно збільшується у геометричній прогресії. Навіть попри війну, Україна розпочала оцифрування багатьох державних сервісів. Тобто відбулася цифровізація державних послуг, переведення їх в режим онлайн, що, у свою чергу, стало ефективним інструментом у надскладних умовах сьогодення.

На цьому фоні Україна продовжує героїчно боротися за свої території і тримати оборону на кіберфронті, який працює у режимі 24/7. Крім виявлення та запобігання кібератакам на українські ресурси, кібер добровольці надають гідну відсіч противнику: щотижня атакують більше сотні онлайн-ресурсів, пов’язаних з рф та їхніми сервісами для бізнесу. Реалізують DDoS-атаки, які призводять до збою в інформаційних системах рос-ЗМІ та навіть зупиняють деякі підприємства військово-промислового комплексу. Проте, на перманентній основі, спецслужби рф, маючи у своєму розпорядженні армію хакерів та кіберзлочинців, все частіше здійснюють поширення шкідливого програмного забезпечення з метою нівелювання авторитету української влади в інформаційній сфері, пошкодження або знищення комп’ютерних мереж органів державної влади, місцевого самоврядування й об’єктів критичної інфраструктури. Тому висвітлення питань, присвячених особливостям застосування та використання шкідливого програмного забезпечення спецслужбами країни-агресора, набуває неабиякої актуальності в сучасних реаліях та потребує подальшого дослідження.

Результати аналізу наукових публікацій. Розгляд проблемних питань щодо форм та змісту шкідливого програмного забезпечення здійснювали: О. Волков [1], О.П. Войтович, М.В. Гурський, Л.М. Куперштейн, Д.С. Сніговий [2], І.А. Терейковський [5]. Деякі питання судово-експертного та методологічного дослідження шкідливих програмних засобів у рамках протидії кібертероризму та кіберзлочинності аналізували у своїх працях: Б.Д. Леонов та В.С. Серьогін [3], О.А. Парфило та Ю.Ю. Нізовець [4], О.А. Самойленко [6] та інші фахівці. Проте залишаються недостатньо висвітленими особливості застосування та використання спецслужбами держави-агресора шкідливого програмного забезпечення на шкоду національній безпеці України в умовах кібервійни.

Метою статті є висвітлення особливостей використання та застосування шкідливого програмного забезпечення хакерами та кіберзлочинцями на замовлення спецслужб країни-агресора, обґрунтування передумов та механізмів виявлення та блокування шкідливого програмного забезпечення, яке системно поширюють хакери та кіберзлочинці у вітчизняному сегменті кіберпростору.

Виклад основного матеріалу. В сучасних умовах відбувається масштабне поширення передових цифрових інформаційних технологій, які впроваджуються в сучасні реалії та використовуються на комп’ютерах, гаджетах, мобільних пристроях

громадян, підприємств, установ, організацій, у тому числі й державного сектора, у зв'язку з чим усі вказані категорії є залежними та певним чином уразливими до фішінгових атак, які використовують для цього Інтернет як транспортну мережу. Атаки здійснюються на усіх користувачів мережі Інтернет. Загальновідомо, що проблематика поширення шкідливого програмного забезпечення існує досить тривалий час, не одне десятиріччя. Україна зазнає кібератак із використанням шкідливого програмного забезпечення різної потужності, починаючи ще з 2014 року.

До загальновідомого шкідливого програмного забезпечення (malware) експерти відносять будь-яке програмне забезпечення, яке несанкціоновано проникає в комп'ютерну техніку або до переферійних пристроїв. В основі шкідливого програмного забезпечення знаходяться програми, які мають за мету спричинення шкоди або виведення з ладу певного програмного пристрою або мережі. Кіберзлочинці, зазвичай, використовують їх з метою доступу до даних, які у свою чергу, можуть використовуватися задля отримання фінансової або іншої вигоди від жертв. Кінцевою метою поширення шкідливих програм може бути викрадання певної інформації, у тому числі й персональних даних певного користувача, зараження комп'ютерів вірусами, примусове взяття управління над певною кількістю комп'ютерів для запуску DDos-атак, спрямованих проти інших мереж тощо. З моменту свого виникнення, понад 30 років потому, існує достатньо способів атак шкідливими програмами, зміст яких включає вкладення електронної пошти, шкідливу рекламу на популярних сайтах, встановлення підробленого програмного забезпечення, інфіковані USB-накопичувачі та додатки, фішингові електронні листи та навіть SMS-повідомлення.

Шкідливе програмне забезпечення (далі – ШПЗ) – це програмне забезпечення, яке за умови запуску може завдати шкоди пристрою різними способами, зокрема – призвести до: блокування пристрою та його непридатності для використання; крадіжки, видалення або шифрування даних; використання пристрою для атак на інші пристрої; отримання кіберзловмисниками інформації щодо облікових даних, які дозволяють отримати доступ до систем або служб, які використовуються; застосування з метою незаконного майнингу криптовалюти на вашому пристрої; використання платних послуг на основі ваших даних (наприклад, телефонні дзвінки на платні номери) тощо.

Шкідливе програмне забезпечення – це зловмисна програма або код, які шкодять кінцевим пристроям. Якщо пристрій уражено шкідливим програмним забезпеченням, може відбуватися несанкціонований доступ, ураження даних або блокування пристрою, доки ви не сплатите викуп. Шкідливе програмне забезпечення очолює деякі рейтинги кібератак. Воно може діяти за декількома напрямками: забороняти доступ до мережі, "красти" інформацію з жорсткого диска та порушувати чи виводити з ладу систему. Шкідливе програмне забезпечення може бути у вигляді шпигунських програм, які збирають інформацію для подальшого викупу. Можуть бути спеціально розроблені програми-вимагачі, які шифрують дані користувача і вимагають викуп (зокрема у криптовалюті) за їхнє розшифрування.

Шкідливе програмне забезпечення може розповсюджуватися через віруси (заражають програми), трояни (ховаються всередині корисної програми) та хробаки (поширюються через вкладення електронної пошти). Наразі найпопулярнішим способом незаконного проникнення є фішинг (60-70 % скоєних кібератак були саме фішинговими). Термін "фішинг" (англ. *phishing* – "видобування") – означає вид Інтернет-шахрайства, який полягає в крадіжці конфіденційних даних користувачів. Іншими словами, зловмисники "розводять" користувачів на те, щоб вони самі розкрили свої персональні дані, наприклад, номери телефонів, номери та секретні коди

банківських карт, логіни та паролі електронної пошти та облікових записів в соціальних мережах. Фішинг – це надсилання шахрайських електронних листів, які можуть бути замаскованими під надійне чи офіційне джерело. Фішингові атаки можуть відбуватися через соціальні мережі або інші онлайн-спільноти. Зловмисники можуть заздалегідь збирати інформацію для того, щоб замаскуватися. Головна зброя фішингу – листи. Тому, в першу чергу, варто звертати увагу на адресу відправника. Одна неправильна літера чи навіть крапка має насторожити користувача і стати першим дзвіночком, аби не відкривати дане повідомлення. Користувачі в мережі Інтернет не завжди можуть розпізнати підробку та можуть залишити на шахрайському веб-сайті свої персональні та інші дані. Кіберзлочинці, отримавши таку інформацію про особу, можуть її використовувати, в т.ч. для привласнення її грошей.

Заслуговує на увагу позиція заступника секретаря РНБО України С. Демедюка про те, що з початком повномасштабної військової агресії саме фішинг став одним з напрямів гібридної війни російської федерації проти України. Адже десятки зловмисних груп, які проводять фішингові кампанії проти українських громадян, координуються російськими злочинцями, а російська спецслужба покриває їхні дії. Внаслідок цього кошти, які втрачають українці, використовуються для підтримки країни-терориста. За підсумками 2021 року зловмисникам вдалося заволодіти 200 млн. грн українських громадян. Але це статистика лише щодо тих, хто звернувся до НБУ та повідомив про правопорушення. Як слушно зазначив заступник секретаря РНБО України, реальна цифра втрачених коштів може бути вдвічі більшою [7]. Хоч це парадоксально, навіть під час повномасштабної війни в Україні платіжне шахрайство нікуди не зникло. Навпаки, у 2022 році спостерігалося суттєве збільшення його проявів. Найпоширенішим видом стала фейкова соціальна допомога від державних чи міжнародних організацій постраждалим від війни українцям. У 2022 році НБУ виявив близько 4500 фішингових ресурсів, для порівняння – у 2021 році ця цифра була значно меншою [7]. На цьому фоні, на жаль, в сучасних реаліях в нашій державі на рівні законів відсутні положення, які б містили, в першу чергу, превентивні заходи для користувачів мережі Інтернет, визначали основоположні вимоги та правила протидії фішингу та фішинговим веб-сайтам, встановлювали додаткові обов’язки для постачальників електронних комунікаційних послуг.

Реальною загрозою є встановлення недосвідченими користувачами на своїх мобільних пристроях, гаджетах або смартфонах зловмисного програмного забезпечення, яке може спричинити істотну шкоду або призвести до масштабних збитків організацій або установ, де вони працюють. Кіберзлочинці та хакери можуть отримати доступ до соціальних мереж, особистої та корпоративної пошти певної фізичної або юридичної особи, даних платіжних карток, списку контактів, вимагати гроші, заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, можливості кіберзлочинців постійно збільшуються. Одним із найбільш поширюваних та ефективних програмних засобів, які маскують звернення зловмисників до доменів Інтернету є мережа TOR. Анонімізація трафіку забезпечується за рахунок використання розподіленої мережі серверів на рівні onion-маршрутизаторів, що, у свою чергу, забезпечує маскування вихідних з’єднань, а також захист аналізу трафіку, забезпечуючи практично повну конфіденційність дій у мережі Інтернет. Окрім цього, мережа TOR дозволяє маскувати IP-адреси шляхом пропуску трафіку користувача через проксі-сервер на своєму ПК, який звертається до серверів TOR, періодично утворюючи мережевий ланцюг з багаторівневим шифруванням вихідним пакетом. Кожен такий пакет даних проходить три різноманітних проксі-сервера, які визначаються випадковим чином.

Перед кожним відправленням пакет послідовно шифрується трьома ключами: спочатку для третього мережевого вузла, потім для другого та лише у кінці – для першого. Коли перший вузол отримує пакет, він розшифровує перший рівень зашифрованої інформації та спрямовує мережеві пакети на наступний проксі-сервер. Другий та третій сервер діють аналогічним способом. Вказані проксі-сервери працюють на SOCKS-інтерфейсі, що дає змогу використовувати для підключення до мережі TOR програмні продукти, засновані на такому самому принципі роботи. До такого виду програмного забезпечення можна віднести браузер DuckDuckGO, який дозволяє також залишатися анонімним у мережі. Для більшої надійності злочинці працюють з мережею TOR через з'єднання VPN, яке шифрує Інтернет-трафік з використанням модемів, анонімних сім-карт, підключення до публічних DNS-серверів та інших засобів анонімізації. Для приховування діяльності у мережі, найбільш технічно підготовлені зловмисники реалізують хакерські атаки через клієнтські машини жертв шляхом сканування та використання уразливостей, завантаження на технічні засоби жертви експлойтів, іншого шкідливого програмного забезпечення та інших способів отримання віддаленого доступу. При використанні вказаної схеми встановити особу зловмисника шляхом направлення запиту Інтернет- провайдеру та Інтернет-сервісам не видається можливим, оскільки відповіді, які отримані за міжнародними каналами зв'язку, очікуються досить тривалий період часу. У зв'язку з цим отримання комп'ютерної інформації внаслідок послідовного відправлення запитів власникам серверів, через яких проходив трафік зловмисників, не дає очікуваних позитивних результатів.

Одним із найбільш поширених видів шкідливого програмного забезпечення є бекдор-вірус Glupteba-AFJK, який є підвидом трояна Glupteba. До недавного часу цей вірус за своїм змістом був вірусом-вимагачем, доки не був трансформований та модернізований у бекдор, який надає змогу отримати доступ до комп'ютерної системи у цілях проникнення або впровадження іншого шкідливого програмного забезпечення.

Окрім цього, у якості прикладу можна вказати на розроблений іранською кіберзлочинною групою "CharmingKitten" бекдор PowerLess, який призначений для кібершпіонажу шляхом завантаження в систему через засоби автоматизації. Новий бекдор PowerLess здатний завантажувати та виконувати додаткові модулі, такі як інфостілери та кейлогери, які надають змогу отримувати доступ до облікових записів жертви, даних браузера та фінансової інформації клієнтської машини. Особливість застосування бекдорів полягає у тому, що їх часто неможливо виявити у системі. Це обумовлено тим, що бекдори під час їхнього впровадження в систему автоматично переміщуються в автозавантаження клієнтської машини жертви одночасно із зміною файлів реєстру. Тобто зміст роботи бекдорів полягає у тому, що вони, проникаючи у систему, маскуються під системні файли, яким є, наприклад, файл CL.exe, котрий є засобом управління MicrosoftC++. Практично усі бекдори є резидентними, тобто активними під час роботи системи або під час функціональності певного програмного забезпечення. Ця властивість дає можливість самовідтворюватися шкідливому ПО під час кожного перезавантаження системи, що обумовлено внесенням змін у значеннях регістрів клієнтських машин. При цьому основне призначення бекдорів є створення уразливостей шляхом вбудування дефектів в алгоритми функціонування системи для інтеграції до клієнтської машини жертви інших типів шкідливого ПО щоб, у кінцевому підсумку, отримати доступ до даних, які зберігаються на клієнтських машинах, а також до операційних систем та підключених засобів входу та виходу.

Для розробки та прикладного застосування шкідливого ПО найбільш підходить операційна система на базі Linux. Слід вказати, що більша частина програмних

продуктів, які призначені для сканування та атак клієнтських машин жертв, представлена у вигляді скриптів, написаних на різних мовах програмування, у яких відсутній графічний інтерфейс. Для застосування таких програмних продуктів найбільш сприятливим у використанні є термінали Unix-подібних систем, до яких відноситься операційна система Linux. Таким чином, вказана операційна система є найбільш зручною для створення та прикладного застосування саме шкідливого ПО.

Кібервійна, яка триває з державою-агресором, є суттєвою загрозою та викликом для національної безпеки. Спецслужби рф, на постійній основі, займаються шпигунством в мережі Інтернет, збирають приватну та публічну інформацію, зламують комп'ютерні системи та мережі інших держав, займаються диверсійно-підривною діяльністю, блокують штатну роботу критичної інфраструктури. З огляду на динамічний розвиток новітніх технологій на мобільних пристроях, рівень та масштаби кібервійни постійно вдосконалюється. Таким чином, контроль над вітчизняним сегментом кіберпростору певним чином визначає стан національної безпеки держави. Така ситуація призводить до активізації діяльності хакерів у кіберпросторі, провокує збільшення кількості атак на державні інформаційні ресурси. Російські хакери, насамперед, атакують інформаційні ресурси вітчизняних державних органів, установ та організацій, компанії фінансового сектору та телекомунікацій. Кіберзлочинці можуть полювати як за державними системами, так і за окремими фізичними або юридичними особами.

Наприклад, у 2022 році була помічена активність розсилання листів з інформацією щодо наявності вакансій з метою укомплектування посад на підприємствах оборонної сфери. Листи містили XLS-файл, який був заражений шкідливою програмою під назвою "Cobalt Strike Beacon". Також зловмисники маскуються під державні органи. Наприклад, у червні 2022 року від імені податкової служби розсилалися фішингові листи з повідомленнями про начебто несплату штрафу. Вкладення містило zip-архів, відкриття якого активувало згадану вище програму "Cobalt Strike Beacon". Російські кіберзлочинці спекулюють і на болючих темах війни та навіть ядерного тероризму з метою залякування та прагненням посіяти паніку серед населення. Тому часто вказують у темах листів та назвах вкладень відповідні слова-маркери. Наприклад, була зафіксована кібератака через документ з назвою "Nuclear Terrorism A Very Real Threat.rtf", всередині якого була схована шкідлива програма "CredoMap".

Спецслужби рф цілеспрямовано та масово застосовують шкідливе програмне забезпечення з метою викрадення та знищення службової інформації в органах державної влади та місцевого самоврядування, у зв'язку з чим ними на постійній основі розробляються відповідні програми. ФСБ за допомогою армії хакерів з використанням шкідливих програм має за мету спричинити масштабні збитки, вразити та заблокувати комп'ютерні мережі органів державної влади, місцевого самоврядування та вивести з ладу об'єкти критичної інфраструктури. Хакери використовують нові розробки шкідливого програмного забезпечення для атаки не тільки на державний сектор, але і на український бізнес.

За попередженням Держспецзв'язку, російські хакери та спецслужби додають до зламаного програмного забезпечення, що розміщуються на торентах, особливий шкідливий код. При цьому хакери троянізують ISO та установчі файли й розміщують їх у безкоштовному доступі на торент-трекерах. Якщо потенційна жертва передбачливо завантажує та встановлює такі файли на свій гаджет або комп'ютер, хакери отримують доступ до його вмісту і можуть протягом тривалого часу залишатися непомітними. Така критична ситуація пояснюється тим, що чимала кількість системних адміністраторів ще й досі використовують неліцензійне програмне забезпечення (в тому числі операційні

системи) в установах та компаніях різних форм власності, що розповсюджується за допомогою торент-трекерів. Встановлюючи зламане або інфіковане ПЗ із торентів, вони фактично надають доступ російським спецслужбам до вмісту робочих машин. Особливо небезпечним є використання зламаної операційної системи, адже в такому випадку зловмисники мають повний адміністративний доступ до гаджета або комп'ютера, на якому її встановлено. Таким чином, встановлюючи неліцензійне програмне забезпечення з неофіційних джерел, торентів користувачі перебувають у зоні підвищеного ризику [8].

Останнім часом російські хакери демонструють чималу активність у вітчизняному сегменті кіберпростору. Російська хакерська група під кодовою назвою TA471 (або UAC-0056), яка підтримує інтереси російського уряду, відзначилася руйнівними кібератаками проти України з використанням нового шкідливого програмного забезпечення "WhisperGate", цілями якої виступають український державний та приватний сектор для організації крадіжок службової та конфіденційної інформації. Зловмисники націлені у першу чергу на Україну, але також періодично атакують країни-члени НАТО в Європі та Північній Америці. Вказана хакерська група TA471 на системній основі поширює інше зловмисне програмне забезпечення для видалення даних. Зловмисне програмне забезпечення маскується під програми-вимагачі, але робить цільові пристрої повністю непрацездатними та нездатними відновлювати файли, навіть якщо виплачується викуп.

Також під час кібератак російські хакери використовують раніше невідоме шкідливе програмне забезпечення для крадіжки інформації під назвою "Graphiron", націлюючись на українські організації. Було встановлено, що зловмисне програмне забезпечення використовувалося для викрадення даних з інфікованих комп'ютерних систем у період з жовтня 2022 року до середини січня 2023 року. Новина про нову шпигунську кампанію TA471 з'явилася через кілька днів після того, як український уряд повідомив про іншу російську хакерську групу під назвою UAC-0010, яка продовжує кібератаки проти українських організацій [9].

Таким чином, держава-агресор активно використовує удосконалене шпигунське програмне забезпечення, наприклад шкідливий носій "EvilGnome", який здатний робити скріншоти, викрадати файли, записувати звук з мікрофону тощо. У свою чергу, "EvilGnome" містить п'ять додаткових шкідливих модулів. Дослідники знайшли зв'язок між "EvilGnome" та хакерським угрупованням "Gamaredon", які тісно пов'язані із рф. Оскільки антивірусні програми та системи безпеки не можуть своєчасно виявити шкідливе ПО "EvilGnome", то експерти рекомендують користувачам комп'ютерів на базі Linux блокувати IP-адреси відповідних серверів. Хакерське шпигунське угруповання "Gamaredon", яке також відоме як "Primitive Bear", діє щонайменше з 2013 року й орієнтується на національні установи, зокрема українські. За масштабами атаки та залученими ресурсами "Gamaredon" – це велика організована професійна група з державною підтримкою рф. У 2019 році вона стала найактивнішою групою проти нашої держави. "Gamaredon" із середини жовтня 2019 року почала атакувати українські установи, окремих дипломатів, військових і правоохоронців, журналістів та різноманітних держслужбовців. Зловмисники доправляли шкідливу програму шляхом цільового фішингу з прикріпленими до листів шкідливими документами. Влітку 2020 року ця структура почала активно використовувати нові інструменти, які включають модуль для Microsoft Outlook, який утворює для користувача електронні листи зі шкідливими документами і відправляє їх контактам жертви.

Тобто для вітчизняного сегменту кіберпростору небезпечним та загрозливим залишається діяльність хакерських угруповань, серед яких найбільшу загрозу несе

“Gamaredon”. Фахівці виявили загрозливу тенденцію до модернізації програмних засобів кібератак із метою підвищення ефективності подолання засобів захисту та приховування своєї діяльності в скомпрометованих системах. Пояснюється це тим, що під час останніх спроб атак використовуються шкідливі вкладення, які імітують документи державних органів влади, зокрема, Служби безпеки України. Хакери розсилають шкідливі документи електронною поштою. Якщо їх відкрити, злочинці отримають доступ до систем та відповідних мереж. Отже, потужні кібератаки, фейкові протести, агентурні мережі та дезінформація є саме тими інструментами, які використовує рф для того, щоб тримати Україну у постійній напрузі.

Останнім часом, фахівці фіксують динамічне зростання кількості кіберінцидентів і кібератак на державні інформаційні ресурси та об’єкти критичної інфраструктури України. За час повномасштабної війни росіяни неодноразово вчиняли хакерські атаки на українські та інші європейські сайти. Основною метою хакерів є кібершпигунство, порушення доступності державних інформаційних сервісів та знищення даних інформаційних систем. Фахівці Державного центру кіберзахисту фіксують динамічне істотне зростання розповсюдження шкідливого програмного забезпечення, яке дає можливість хакерам викрадати дані чи й взагалі знищувати їх. Кількість атак із високим рівнем критичності зросла у 3,8 раза, а кількість зареєстрованих кіберінцидентів із високим рівнем критичності – на 128 %. При цьому кількість критичних подій інформаційної безпеки, джерелом яких є IP-адреси рф зросла у 35 разів. Саме з IP-адреси рф здійснювали кібератаки на українські інформаційні ресурси, а також розповсюджували фейки. Абсолютна більшість кіберінцидентів пов’язана з хакерськими угрупуваннями, яких фінансує російська влада, як-от UAC-0010 (Armageddon) та інші.

Урядова команда реагування на комп’ютерні надзвичайні події України “CERT-UA”, яка діє при Державній службі спеціального зв’язку та захисту інформації (Держспецзв’язку), зафіксувала поширення серед державних органів небезпечних електронних листів на тему “Інформація про військових злочинців рф”. Електронний лист містить HTML-файл “Військові злочинці рф.htm”, відкриття якого призведе до створення на комп’ютері RAR-архіву “Viyskovi_zlochinci_RU.rar”. Згаданий архів містить файл-ярлик “Військові-злочинці, які знищують Україну (домашні адреси, фото, номери телефонів, сторінки в соціальних мережах).lnk”, відкриття якого призведе до того, що зловмисники отримають віддалений доступ до комп’ютера жертви. У “CERT-UA” зазначають, що це розсилання асоційоване з діяльністю хакерської групи “UAC-0010” (Armageddon).

Протягом тривалого часу російська агентура під керівництвом кураторів ФСБ рф встановлювала через українські комерційні структури шпигунський софт на комп’ютери та мобільні термінали шляхом безпосереднього та віддаленого доступу під виглядом DLP-систем, програм контролю якості роботи співробітників підприємств тощо. Шпигунське програмне забезпечення російського походження активно використовувалося з метою негласного отримання інформації з комп’ютерних мереж підприємств військово-промислового комплексу, органів виконавчої влади, об’єктів критичної інфраструктури тощо.

У 2022 році ФСБ рф створило шкідливе програмне забезпечення для Android, замаскувавши його під додаток “Cyber Azov”. Дослідники з компанії “Google” виявили шкідливе програмне забезпечення від російської державної групи кіберзлочинців, замасковане під проукраїнський додаток “КіберАзов”, який начебто створив український полк “Азов” для того, щоб “допомогти зупинити російську агресію проти України”. Насправді ж воно належить російській хакерській групі “Turla”. Злочинне

угрупування, яке підпорядковане ФСБ рф, пов'язують з атаками на європейські та американські організації за допомогою шкідливих програм [10].

Після тривалих невдач на полі бою росіяни на системній основі посилюють та удосконалюють кібератаки на цивільну інфраструктуру, електроенергетику, об'єкти стратегічних галузей економіки та транспорту тощо. Хоча Росія більше покладалася на ракетні удари, ніж на кіберзброю для досягнення своїх цілей в Україні, напади на групи енергетичної, урядової та транспортної інфраструктури переконливо демонструють, що кібератаки все ще є ключовою частиною загальної стратегії Кремля зломити волю та бойовий дух українців. До кібератак рф вдавалася ще від початку повномасштабного вторгнення. Однак, якщо раніше вони були спрямовані здебільшого на військові цілі, то в сучасних реаліях хакери активно націлилися на критичну інфраструктуру.

Тільки за 2022 рік українські організації та установи пережили понад 2000 кібератак. Понад 300 з них були спрямовані на безпековий і оборонний сектор, більш ніж 400 – на цивільне життя, включно з комерційними, енергетичними, фінансовими і телекомунікаційними компаніями. Ще понад 500 атак припали на урядові об'єкти. Від початку повномасштабної війни і станом на середину листопада 2022 року на українську енергетику було здійснено 1,2 млн. кібератак, а за весь 2021 рік таких нападів було 900000 [11]. Влітку 2022 року російські хакери атакували ІТ-інфраструктуру групи ДТЕК. Мета зловмисників – дестабілізувати технологічні процеси генеруючих та розподільчих компаній та підірвати енергетичну безпеку України, а також поширити через пропагандистські канали явну неправдиву інформацію про роботу компаній та, як наслідок, залишити без електропостачання українських споживачів. Хакерську атаку було проведено одночасно з ракетним обстрілом Криворізької ТЕС [12].

Проте російські хакери атакують не тільки Україну. У 2022 році російські хакери вивели з ладу декілька норвезьких урядових сайтів і сервісів, назвавши це помстою за обмеження Норвегією традиційного маршруту транзиту вантажів рф на архіпелаг Шпіцберген [13]. У листопаді 2022 року через масштабну російську кібератаку в Естонії тимчасово стали недоступними електронні канали консорціуму "Eesti Energia". Російські хакери намагалися зламати веб-ресурси компанії та застосунки "Elektrilevi MARU". Крім цього, під удар потрапили компанії в Латвії та Польщі. Також хакерського нападу зазнали Міністерство економіки, Банк Естонії та фонд EAS. Доступ до клієнтських каналів і решти ресурсів поступово відновили. [14].

У січні 2023 року королівську пошту Великобританії атакував вірус-вимагач, який пов'язують з російськими кіберзлочинцями. За наслідками кібератаки поштова служба Великобританії не була спроможна надсилати посилки та листи за кордон протягом тривалого часу. За результатами нападу постраждали комп'ютерні системи, які використовувалися для обробки та відстеження поштових відправлень за кордон. Вірус потужно вразив програмне забезпечення у шести офісах пошти, зокрема, у центрі обробки у Хітроу біля Лондона. Хакери нібито попросили викуп у розмірі кілька мільйонів фунтів, проте фахівці заявили, що можуть повернути системи до роботи і без виплати. Хакерські атаки із застосуванням вірусів-здирників відбуваються в різних країнах світу майже щодня, проте напад на Королівську пошту – особливий випадок, оскільки вона належить до об'єктів критичної інфраструктури країни, тобто є вкрай важливою для британської економіки. Під час нападу було застосовано програму-вимагач "Lockbit", розробниками якої є злочинні групи, пов'язані з рф [15]. У 2022 році влада США звинуватила в організації хакерської атаки за допомогою програми-вимагача "Lockbit" особу з подвійним канадсько-російським громадянством, при цьому хакер діяв із території Канади.

Російська хакерська група, відома під назвою “Cold River”, влітку 2022 року атакувала три лабораторії ядерних досліджень у США. У період з серпня по вересень 2022 року “Cold River” завдала ударів по Брукхейвенській (BNL), Аргонській (ANL) і Ліверморській національній лабораторії імені Лоуренса (LLNL). Атака проти американських лабораторій сталася приблизно в той самий час, як експерти МАГАТЕ прибули до України, щоб відвідати Запорізьку АЕС, яка зараз перебуває в окупації [16].

Національний центр кібербезпеки (NCSC) Великобританії видав офіційне застереження про те, що російські та іранські хакери намагаються зламати листування та облікові записи відомих британців. Декілька груп хакерів розгорнули шпигунське полювання насамперед на політиків, чиновників, журналістів, аналітиків та громадських діячів. Хакери шпигують за потенційними жертвами в соцмережах, вони можуть підробити облікові записи і видати себе за реальний контакт жертви, використовуючи особисту пошту. Вони можуть надсилати фальшиві запрошення з вірусом на конференції та заходи або навіть на зустрічі у “Zoom”. Якщо на них клікнути, шкідливий код дозволить хакеру отримати доступ до облікових записів і, можливо, делікатної інформації. Зламаний обліковий запис використовують для того, щоб вступити в контакт з новою жертвою. Хакери здебільшого цікавляться тими, хто досліджує проблематику Ірану та Росії чи іншим чином пов’язаний із цими країнами. Російське угруповання, відоме під назвами “Cold River” та “Seaborgium”, звинувачують, зокрема, у зламі електронної пошти колишнього керівника британської розвідки MI6 Річарда Дірлава. Хакери “Cold River” атакували низку громадських організацій та аналітичних центрів у США, військові центри кількох східноєвропейських країн, військове підприємство в Україні та один із навчальних центрів НАТО [17].

Шкідливі програми, які поширюють хакери та кіберзлочинці на замовлення ФСБ рф, дозволяють отримувати доступ до державних інформаційних ресурсів, конфіденційної інформації, корпоративних систем. За таких умов можна констатувати певні труднощі у виявленні загроз, що свідчить про складність моніторингу та контролю вбудованого ПЗ. Проблема також ускладнюється такими факторами як, недостатня обізнаність та проблема автоматизації. Вбудоване програмне забезпечення стає пріоритетною мішенню для хакерів, адже в ньому зберігається конфіденційна інформація, як-от облікові дані та ключі шифрування.

Нещодавно Національний інститут стандартизації і технологій (NIST) засвідчив більш ніж п’ятикратне збільшення кількості атак на вбудоване програмне забезпечення за останні чотири роки. При цьому рівень обізнаності про цю загрозу відстає від інших галузей. Такий сплеск кількості атак на прошивки дослідження, на думку експертів, демонструє, що уразливості в ПЗ втричі частіше створюють загрозу порівняно з вразливостями в мікропрограмах. Відсутність автоматизації є ще одним фактором, який змушує організації втрачати час, який можно було б використати для розробки більш ефективних стратегій превентивного захисту. 71 % опитаних фахівців стверджує, що їхні співробітники витрачають занадто багато часу на роботу, яка може і має бути автоматизована. Загалом команди фахівців з інформаційної безпеки витрачають 41 % свого часу на процес відновлення.

Вбудоване програмне забезпечення керує апаратним обладнанням, але воно на 100 % не захищено. Кібератаки на вбудоване програмне забезпечення менш поширені, ніж на програмне забезпечення, але успішна атака буде більш руйнівною. Таким чином, державний та приватний сектор повинні мати більш проактивні стратегії в галузі кібербезпеки, особливо коли мова йде про боротьбу з атаками на вбудоване програмне забезпечення. Шкідливі програми, призначені для заподіяння шкоди та використання

ресурсів персональних комп'ютерів, включають: вимагачі, трояни, макровіруси, логічні бомби. Зазвичай їх використовують для отримання будь-яких конфіденційних даних: від фінансових показників, до паролів, медичних записів чи особистого листування тощо.

За останніми експертними спостереженнями, автори програм-вимагачів дедалі більше відходять від тактик безадресної атаки на користь високобюджетних цілей, для чого організовують збір інформації про майбутню жертву до того, як почати безпосереднє інфікування. Такі групи кіберзлочинців можуть тижнями чи місяцями збирати інформацію в інфікованих системах та лише після цього розгортати програми-вимагачі. Таким чином, деякі кіберзлочинці намагаються отримати надприбуток, інші – ставлять мету підірвати довіру пересічених громадян до державних установ.

Також російськими хакерами широко використовуються так звані SQL-ін'єкційні атаки (або "довгий рядок") чи той самий брутфорс. Цей тип атак призначений для ураження веб-сайтів, що працюють на основі баз даних. В основі методу – використання шкідливого SQL коду для маніпуляцій з базою даних на сервері з метою отримати доступ до інформації, яка мала б залишатися прихованою. Успішна SQL-ін'єкційна атака може надати у розпорядження хакерів паролі та особисту інформацію, змінити дані, які зберігаються в базі, виконувати адміністративні операції, відновлювати вміст файлів та, навіть, надавати команди операційній системі. Ще одним видом кібератаки є міжсайтовий скриптинг (XXS), який реалізується, коли через сторінки, які були згенеровані сервером, потрапляють користувацькі скрипти. Специфіка подібних атак полягає в тому, що замість безпосередньої атаки сервера зловмисники використовують вразливий сервер для атаки на користувача. У підсумку разом із веб-сторінкою, яку завантажує жертва, вона отримує зловмисний код, інтегрований в HTML. Цей код продовжує виконувати шкідливий сценарій на комп'ютері жертви, наприклад, шляхом надсилання хакерам файлів cookie з персональними даними користувача.

Також актуальним з позиції поширення шкідливого програмного забезпечення залишається фішинг, який існує протягом багатьох років і має широкий спектр методів інфікування жертв. Найчастіше зловмисники видають себе за банки або інші фінансові установи для того, щоб змусити жертву заповнити фальшиву форму й отримати персональні дані. Раніше для виманювання даних користувачів кіберзлочинці часто використовували неправильно написані або помилкові доменні імена. На сьогодні зловмисники використовують більш складні методи, завдяки чому фальсифіковані сторінки досить схожі на свої законні аналоги. Спроби хакерів отримати доступ до IT-інфраструктури державного органу або певної компанії та заволодіти конфіденційними даними є реальними. Майже неможливо гарантувати повноцінний захист від усіх типів нападів. Більшість кібератак здійснюється зловмисниками продумано та заздалегідь. Вони готуються і використовують для цього спеціальне програмне забезпечення. Щоб попередити та знизити можливі ризики, доцільно посилювати кібербезпеку на усіх рівнях.

Небезпеку для інформації несуть і відкриті Wi-Fi мережі, адже кожен має змогу до них підключитися та виконати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись, прочитавши пароль з чеку чи дізнавшись його у працівника. Тому ці проблеми захисту інформації в бездротових мережах є актуальними та поширеними. Ненадійні паролі зазвичай стають причиною хакерських атак. Після того як зловмисник підключиться до мережі, він зможе отримати доступ абсолютно до всіх підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі пристрої також піддаються ризику хакерської атаки. Хакери можуть запустити шкідливий код на майже будь-якому гаджеті через вразливість Wi-Fi.

При цьому небезпечність атаки полягає у тому, що зловмисник може впровадити шкідливий код JavaScript жертві в незашифрованих HTTP-з'єднаннях з метою використання вразливостей у браузері жертви.

Так, кіберфахівці вітчизняної спецслужби у січні 2023 року нейтралізували російську хакерську атаку на електронні системи житлової інфраструктури в одному з прикордонних регіонів України. Через Wi-Fi мережу багатоквартирних будинків хакери прагнули дистанційно підключитись до системи відеоспостереження за територією житлових комплексів, прилеглими автомобільними дорогами тощо. Таким чином, вони планували мати прихований канал для збору інформації про ситуацію в місті. Також агресора цікавили відомості щодо адрес проживання українських правоохоронців та можливого переміщення військової техніки. За оперативними даними, до кібератаки причетне підконтрольне російським спецслужбам хакерське угруповання, яке спеціалізується на зламах електронних систем інфраструктурних об'єктів [18]. Виходячи із ризиків та загроз у кіберпросторі, які поширюють російські хакери, Україна увійшла до складу міжнародної групи, яка боротиметься з програмами-вимагачами [19].

23 січня 2023 року розпочала роботу міжнародна група, яка консолідує зусилля світової спільноти задля боротьби з програмами-вимагачами. Група працює у межах ініціативи під керівництвом США "Counter Ransomware Initiative", до складу якої входять уряди 37 країн, зокрема України. Очікується, що діяльність цієї міжнародної структури гарантовано забезпечить стійку та ефективну світову співпрацю, спрямовану на припинення, запобігання та захист від зростаючої глобальної загрози, пов'язаної із поширенням програмам-вимагачів. Створення цієї групи було погоджено з членами Ініціативи на зустрічі у Вашингтоні в листопаді 2022 року. Її учасники будуть обмінюватися інформацією та розвідувальними даними, досвідом у галузі політики та правових структур, а також співпрацюватимуть правоохоронні органи країн-учасниць. Оскільки програми-вимагачі становлять глобальну загрозу, то інституційне забезпечення заходів щодо ефективного виявлення та переслідування кіберзлочинців, які використовують програми-вимагачі для отримання фінансової та іншої вигоди є одним із важливих пріоритетів міжнародного співробітництва за участю України.

15 лютого 2023 року Національний координаційний центр кібербезпеки (НКЦК) при РНБО України спільно з Національним банком анонсували запуск автоматичної централізованої системи Protective DNS, яка має протидіяти кібершахрайству у фінансовому секторі. Ще наприкінці 2022 року її успішно протестували. На сьогодні до системи вже приєдналися найбільші українські телеком- та Інтернет-провайдери, зокрема Kyivstar, lifecell, Vodafone, "Укртелеком", "Датагруп" і "Воля". Стратегічне завдання цього проєкту – зменшити переходи користувачів на шахрайські сайти шляхом перенаправлення їх на сторінку з попередженням, що сайт створений зловмисниками. Регулятором – Національною комісією, яка здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв`язку (НКЕК) доведено до відома постачальників електронних комунікаційних мереж та послуг розпорядження Національного центру оперативно-технічного управління мережами телекомунікацій (НЦУ) від 30.01.23 р. № 67/850 про впровадження системи фільтрації фішингових доменів [20].

Висновки.

Серед найвідоміших видів шкідливого програмного забезпечення – віруси, трояни, програми-вимагачі, хробаки та інші. Шкідливе програмне забезпечення може поширюватися шляхом: електронних листів із небезпечними вкладеннями або посиланнями; експлуатації зловмисником вразливостей систем; флеш-носії; використання

неліцензійних копій програмного забезпечення; завантаження програмного забезпечення з неофіційних ресурсів; фішингу тощо. Зміна зловмисниками IP-адрес, MAC-адрес клієнтських машин, а также використання інших способів анонімізації у мережі зводить нанівець пошук та виявлення вказаних осіб, які використовують шкідливе ПО на системній основі. За півтора роки війни масштаби поширення шкідливого програмного забезпечення російського походження значно зросли. Ескалація у кіберпросторі триває. Світова тенденція сучасності – кожна країна динамічно працює над інституційними засадами створення кібервійськ, навіть в певних випадках у форматі створення організованої армії хакерів під державним прапором. На російський уряд та спецслужби рф працюють чисельні групи хакерів та кіберзлочинців, які на замовлення ворога виконують злочинні вказівки Кремля навколо світу, хоча у фокусі їхньої прискіпливої уваги переважно Україна. На переконання багатьох західних експертів, саме російський уряд є світовим лідером, який опікується організацією хакерських кібератак та кібершпигунством. Масштабування хакерських атак та активізація діяльності кіберзлочинців, які виступають під російським прапором, очікувано буде збільшуватися, особливо в умовах триваючої кібервійни.

У другій половині 2023 року Україна очікувано вступає у нову фазу кібервійни в рамках потужного протистояння у кіберпросторі, захист якого є важливою складовою національної безпеки. Передбачається збільшення кількості російських кібератак на фоні нових поразок держави-агресора на полі бою. Окрім можливих кібератак проти України, у фокусі уваги російських хакерів та кіберзлочинців залишається несанкціонований доступ до важливих державних та комерційних інформаційних ресурсів, конфіденційної або службової інформації, виведення з ладу та блокування роботи об’єктів критичної інфраструктури, переважно енергетики на території України, а також держав-членів НАТО, що також є цілком реальним та прогнозованим.

Враховуючи викладене, важливим залишається розробка Стратегії управління ризиками, пов’язаними із поширенням шкідливого програмного забезпечення. Також доцільним вбачається прискорити схвалення Закону України “Про внесення змін до Закону України “Про електронні комунікації” (щодо протидії фішингу)”, проект якого (від 28.04.23 р. № 9250) перебуває на розгляді Верховної Ради України [21], що надасть змогу на державному рівні посилити системну боротьбу з фішингом та фішинговими вебсайтами, запровадити відповідні правила протидії фішингу та фішинговим вебсайтам, встановити права та обов’язки постачальників DNS. Прийняття вказаного закону є конче необхідним для вирішення питань протидії фішингу, в першу чергу, протидії кіберзлочинцям, які виманюють інформацію у користувачів в мережі Інтернет про їх дані у банківських та фінансових установах. Запропонований законопроект вводить в законодавчий обіг такі поняття, як “фішинг” та “фішинґовий веб-сайт”, а також містить положення, спрямовані на системну протидію фішингу та фішинговим вебсайтам шляхом надання повноважень центральному органу виконавчої влади у сферах електронних комунікацій та радіочастотного спектра з розробки (на підставі пропозицій Національного банку України) правил протидії фішингу та фішинговим веб-сайтам.

Використана література

1. Волков О.О. Поняття шкідливого програмного засобу, призначеного для несанкціонованого втручання в роботу електронно-обчислювальної техніки. *Науковий вісник Національної академії внутрішні справ.* 2018. № 1 (106) С. 217-231.

2. Войтович О.П. Гурський М.В., Куперштейн Л.М., Сніговий Д.С. Засіб моніторингу для операційної системи Android. *Вісник Хмельницького національного університету. Технічні науки*. 2017. № 3. С. 236-241.

3. Парфило О.А., Нізовець Ю.Ю. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму. *Криміналістичний вісник.* 2016. № 1 (25). С. 78-84.

4. Леонов Б.Д., Серьогін В.С. Методичне забезпечення заходів класифікації, ідентифікації та фіксації кіберзлочинів. *Інформація і право*. № 1(36)/2021. С. 99-105.

5. Терейковський І.А. Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення. *Безпека інформації.* 2013. Т. 19. № 1. С. 24-28.

6. Самойленко О.А. Протидія кіберзлочинам: криміналістичний аспект: навчально-методичний посібник. Одеса, 2020. 133 с.

7. В Україні запустили проект із протидії кібершахрайству у фінансовому секторі. URL: https://www.ukrinform.ua/rubric-economy/3670375-v-ukraini-zapustili-proekt-iz-protidii-kibersahraj stvu -u-finansovomu-sektori.html

8. Російські хакери розповсюджують заражене програмне забезпечення через торенти. URL: https://cip.gov.ua/ua/news/russian-hackers-spread-infected-software-through-torrents

9. Російські хакери використовують нове шкідливе програмне забезпечення для атаки на українські компанії. URL: https://fintechinsider.com.ua/rosijski-hakery-vykorystovuyut-nove-shkid lyve-programne-zabezpechennya-dlya-ataky-na-ukrayinski-kompaniyi

10. Російські хакери створили фейковий застосунок "КіберАзов" – (Google). URL: https://texty.org.ua/fragments/107305/rosijski-hakery-stvoryly-fejkovyj-zastosunok-kiberazov-google

11. Російські хакери посилюють кібератаки на цивільні цілі, щоб тероризувати українців, – посадовець АНБ. URL: https://lb.ua/society/2023/01/12/542313_rosiyski_hakeri_posilyuyut.html

12. Російські хакери атакували ІТ-інфраструктуру групи ДТЕК. URL: https://biz.liga.net/ ua/ekonomika/it/novosti/rossiyskie-hakery-atakovali-it-infrastrukturu-gruppy-dtek

13. Російські хакери почали кібератаки проти Норвегії за обмеження транзиту на Шпіцберген. URL: https://www.eurointegration.com.ua/news/2022/06/29/7142248

14. Російські хакери атакували сайти енергетичних підприємств Естонії. URL: https://detector. media/infospace/article/205141/2022-11-20-rosiyski-khakery-atakuvaly-sayty-energetychnykh-pid pryi emstv-estonii

15. Королівську пошту Великобританії атакував вірус-вимагач, який пов'язують з російськими хакерами. URL: https://lb.ua/world/2023/01/13/542399_korolivsku_poshtu_velikobritanii.html

16. Російські хакери атакували три ядерні лабораторії в США – (Reuters). URL: https://www.unian.ua/world/rosiyski-hakeri-atakuvali-tri-yaderni-doslidnicki-laboratoriji-v-ssha-reuters

17. Російські та іранські хакери полюють у соцмережах на відомих британців. URL: https://lb.ua/world/2023/01/26/543772_rosiyski_iranski_hakeri_polyuyut.html

18. СБУ нейтралізувала спробу російських хакерів проникнути у комп'ютерні мережі багатоквартирних будинків. URL: https://ssu.gov.ua/novyny/sbu-neitralizuvala-sprobu-rosiiskykh-kh akeriv-pronyknuty-u-kompiuterni-merezhi-bahatokvartyrnykh-budynkiv

19. Україна увійшла до складу міжнародної групи, яка боротиметься з програмами-вимагачами. URL: https://lb.ua/world/2023/01/24/543494_ukraina_uviyshla_skladu.html

20. Про впровадження системи фільтрації фішингових доменів: Розпорядження НЦУ від 30.01.23 р. № 67/850. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2580&language =uk

21. Про внесення змін до Закону України "Про електронні комунікації" (щодо протидії фішингу): проект закону України від 28.04.23 р. № 9250. URL: https://itd.rada.gov.ua/billInfo/ Bills/Card/41815

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~