Інформаційна і національна безпека

УДК 342.951

ПОЛЯКОВ О.М., начальник відділуУкраїнського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України.
ORCID: https://orcid.org/0000-0002-8984-1476.

СУЧАСНІ ТРЕНДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ЗАСТОСУВАННЮ ШПИГУНСЬКИХ ТА ШКІДЛИВИХ ПРОГРАМ

DOI.....

Анотація. *Визначено масштаби діяльності російських хакерів та кіберзлочинців у глобальному вимірі. Розкрито цілі та завдання злочинних посягань російських хакерів з використанням шпигунського та шкідливого програмного забезпечення. Деталізовано особливості кібератак, які проводять російські хакери та кіберзлочинці. Висвітлено технічний аспект виявлення, блокування та протидії масштабному застосуванню шпигунського та шкідливого програмного забезпечення у мережах в умовах кібервійни. Узагальнено загрози та ризики використання штучного інтелекту під час кібератак. Наведено приклади новітніх розробок щодо впровадження шпигунського та шкідливого програмного забезпечення. Акцентовано увагу на особливостях шкідливого програмного забезпечення "Wiper". Деталізовано проблемні питання сучасного нормативного забезпечення впровадження у нашій державі системи фільтрації фішингових доменів. Висвітлено людський фактор припинення злочинної діяльності хакерів, який передбачає їх фізичне затримання, арешт зловмисників та їх кримінальне переслідування. Охарактеризовані зміст та напрями кіберсуперництва в умовах кібервійни. Визначено перспективи та надано прогноз очікуваної злочинної діяльності російських хакерів та кіберзловмисників у 2023 році. Запропоновано пріоритети щодо боротьби із наслідками поширення шкідливого та шпигунського програмного забезпечення в умовах кібервійни.*

Ключові слова: *шкідливе програмне забезпечення, шпигунське програмне забезпечення, кібербезпека, кіберзахист, кібератака, фішинг, програмне забезпечення, електронні комунікаційні мережі, національна безпека, спецслужба, Хмарні технології, хакерські угрупування, кіберсуперництво, медіаграмотність, штучний інтелект, кібервійна*

Summary*. The scope of activities of the Russian hackers and cybercriminals in the global dimension has been determined. The goals and tasks of the criminal encroachments of Russian hackers using spyware and malicious software have been revealed. The specifics of cyberattacks carried out by Russian hackers and cybercriminals are detailed. The technical aspect of detecting, blocking and countering the large-scale use of spyware and malicious software in networks in the context of cyber warfare is covered. The threats and risks of using artificial intelligence during cyber attacks are summarized. The examples of the latest developments in the implementation of spyware and malware are given. Attention is focused on the features of the "Wiper" malicious software. The problematic issues of modern regulatory support for the implementation of the fishing domain filtering system in our country are detailed. The human factor of stopping the criminal activity of hackers, which involves physical detention, arrest of perpetrators and criminal prosecution, is highlighted. The content and the directions of cyber rivalry in the conditions of cyber warfare are detailed. The perspectives of the expected criminal activity of Russian hackers and cybercriminals in 2023 are provided. Priorities for combating the consequences of the spread of malicious and spy software in the context of cyber warfare are proposed.*

Keywords*:malware, spyware, cyber security, cyber defense, cyber attack, fishing, software, electronic communication networks, national security, intelligence service, cloud technology, hacker groups, cyber rivalry, media literacy, artificial intelligence, cyber warfare.*

Постановка проблеми. Російська Федерація – глобальна світова загроза. Знаковою датою стало 17 березня 2023 року – день, коли Міжнародним кримінальним судом було видано ордер на арешт диктатора Путіна та його поплічників. Розуміючи істерію Кремля з цього приводу, ймовірну та очікувану помсту, масштаби та наслідки російської агресії, провідні держави світу продовжують терміново удосконалювати та модифікувати свої підходи до забезпечення кібербезпеки, спираючись на колосальний досвід російсько-української війни. Так, зокрема 2 березня 2023 року в США набула чинності нова Стратегія кібербезпеки. У свою чергу, держави ЄС активізували зусилля для запуску власної супутникової групи з метою забезпечення безпеки свого урядового зв'язку. Також ці країни інтенсивно працюють над законопроєктом про кіберстійкість (Cyber Resilience Act) у частині підвищення вимог до критичного обладнання на об'єктах критичної інфраструктури та вживають заходів з вдосконалення мережевих стандартів кібербезпеки. Щодо довгострокових наслідків та перспектив, то вже зараз очевидні помітні зміни в східноєвропейській кіберзлочинній екосистемі, де активність російськомовних хакерських спільнот частково знизилася.

В умовах санкційного тиску на рф, ключові світові постачальники комп'ютерних та мережевих послуг залишили ІТ-ринок держави-агресора. Також спостерігається масовий "відтік мізків" з-поміж російських кіберфахівців, які шукають притулку у інших країнах світу для того, щоб не стати жертвами стихійної мобілізації. Найбільш важливий висновок, який можна зробити у цій сфері – російські хакерські групи та кіберзлочинці використовували час для свого навчання та розвитку вмінь, навичок з метою розробки майбутніх алгоритмів та продуманих сценаріїв здійснення потужних та небезпечних кібератак.

За таких умов, висвітлення сучасних трендів виявлення та протидії поширенню шпигунського та шкідливого програмного забезпечення російськими хакерами та кремлівськими ІТ-зловмисниками є актуальним та своєчасним, особливо в умовах ведення кібервійни з державою-агресором та забезпечення виконання обґрунтованих обмежень, які встановлені чинним законодавством в рамках правового режиму воєнного стану в нашій державі.

Результати аналізу наукових публікацій. Питання розробки методологічних засад протидії поширенню шпигунського та шкідливого програмного забезпечення кіберзлочинцями та хакерськими угрупованнями, які суцільно підконтрольні рф, певним чином здійснювали у свої наукових працях: О. Войтович, В. Вітюк, В. Каплун [1], В. Козачок, А. Рой, Л. Бурячок [2], Б. Леонов й В. Серьогін [3], А. Марущак [4], В. Пеньков, Р. Штонда, О. Гук, І. Мальцева, Ю. Черниш [5] та інші фахівці. Проте сучасні напрацювання та розробки методологічного змісту щодо виявлення, блокування та протидії застосуванню шкідливого й шпигунського програмного забезпечення в умовах кібервійни, яку системно веде проти України держава-агресор вказані автори не розглядали, що засвідчує актуальність та своєчасність підготовки цієї наукової статті.

Метою статті є визначення на підставі аналізу новел вітчизняного та зарубіжного законодавства сучасних дієвих й ефективних механізмів виявлення, протидії та блокування шпигунського та шкідливого програмного забезпечення в умовах кібервійни.

Виклад основного матеріалу. На тлі повномасштабного вторгнення російських військ в Україну спецслужби держави-агресора ведуть кібервійну проти України та коаліції держав, які підтримують нашу країну. З початком війни в Україні кібератаки як на національну інфраструктуру, так і на приватні компанії зросли в геометричній прогресії. Також цілями кібератак рф, окрім України, були і залишаються США та Польща, де координується значна частина матеріально-технічного забезпечення військової та гуманітарної допомоги для України. Окрім того, як засвідчує наявний досвід, злочинна діяльність російських хакерів також була спрямована проти країн Балтії. Останнім часом подібні атаки були спрямовані на комп'ютерні мережі Данії, Норвегії, Фінляндії, Швеції, Туреччини та міністерств закордонних справ інших країн НАТО. У другому півріччі 2022 року російські хакери активно атакували логістичні та транспортні компанії, у тому числі й за межами України. Росіяни надають пріоритет урядам країн, але у список цілей для кібератак також потрапляли аналітичні центри, гуманітарні організації, ІТ-компанії, постачальники енергії та інші критично важливі об'єкти інфраструктури. За інформацією міжнародних експертів, кібератаки росіян з початку активної фази війни були успішними лише у 29 % випадків.

З метою узагальнення тактики та особливостей атак найбільш активних російських хакерських угрупувань, Держспецзв'язку підготовлено звіт про кіберагресію рф проти України у 2022 році під назвою "Russians Cyber Tactics: Lessons Learned 2022" [6]. У звіті ретельно досліджено методику та проаналізовано особливості нападів основних хакерських угрупувань, їхню мотивацію, методи та інструменти атак. Ці знання допоможуть у побудові ефективних систем захисту як в українських установах, так і в організаціях по всьому світу. У цьому документі мова йде про стратегічні завдання російських хакерів, оскільки цілі, які стоять перед російськими хакерами, відповідають загальним цілям російської воєнної агресії. Так, експертами Держспецзв'язку підсумовано, що на початку російського вторгнення мішенями для кібератак були медіа та телеком-сфери. Згодом фокус хакерів змістився на енергетичний сектор. На думку фахівців, найнебезпечнішими хакерами з рф є ті, що спеціалізуються на проведенні "тихих операцій", які спрямовані виключно на шпигунські цілі. Зокрема, такі атаки переважно здійснює угруповання "InvisiMole", яке підпорядковане Службі зовнішньої розвідки рф. Їхня злочинна діяльність спрямована на високопосадовців, дипломатів та інших фахівців, які мають доступ до конфіденційної інформації. Оскільки "тихі" атаки складніше виявити, вони можуть мати більш критичні наслідки. Також російські хакери здійснюють кібератаки з метою помсти або для інформаційно-психологічного впливу – для того, щоб переконати населення в тому, що держава не здатна їх захистити. Саме такі атаки привертають до себе увагу ЗМІ та суспільства.

Таргетований фішинг залишається одним із домінантних й ефективних методів отримання доступу до організацій-жертв. Однак у другій половині 2022 року відбулися зміни в тактиці російських хакерів. Замість того, щоб атакувати безпосередньо організації-цілі за допомогою фішингу, хакери почали зміщувати акцент на використання технічних вразливостей установ, які надають послуги операторам критичної інформаційної інфраструктури. Характер атак російських хакерів вказує на те, що жодна установа не може бути в безпеці. Передусім у зоні ризику – компанії, які надають послуги та сервіси операторам критичної інформаційної інфраструктури: розробники, Інтернет-провайдери тощо.

На підставі узагальнення проведеного дослідження можна визначити основні тенденції російської кіберзагрози [6].

Можливо констатувати, що хвиля кібератак, організованих російськими хакерськими угрупованнями, розпочалася ще до початку масштабної війни, тобто до 24 лютого 2022 року.

Перші фішингові кампанії проти України фахівці корпорації "Google" зафіксували ще у квітні 2021 року. У 2022 році кількість кібератак на Україну зросла у 3,5 рази порівняно з 2020 роком, а кількість атак на країни НАТО – учетверо. Аналітики компанії Google прозвітували, що Україну та держави НАТО кібератакують переважно п'ять хакерських угруповань: "FrozenLake", "Coldrive", "Summit, FrozenBarentz" та "FrozenVista", частина з яких співпрацює з ФСБ та ГРУ ГШ рф. Однією із головних стратегій цих хакерських угруповань є фішинг. Найчастіше хакери атакують пошту Gmail, а також поштові сервіси різних урядових установ – Міноборони, МЗС та інших. На переконання провідних експертів, угруповання "FrozenBarentz" пов'язане з ГРУ та армією рф і займається шпигунством, дезінформацією, руйнуванням та знищенням інформаційно-комунікаційних систем. Її підозрюють у здійсненні атак на об'єкти української інфраструктури, які були уражені ще у 2015 та 2016 роках. Об'єктами атак також стали країни НАТО, Грузія та Південна Корея. Крім того, одним з об'єктів кібератак "FrozenBarentz" був турецький виробник безпілотників Bayraktar. Злочинне угруповання "Summit" пов'язане із ФСБ і займається шпигунською діяльністю. Цілями хакерів були переважно сили безпеки країн НАТО. У липні 2022 року кіберзлочинці замаскували шкідливе програмне забезпечення під програму, яку можна завантажити з домену, схожого на сайт полку "Азов" [7].

Російське хакерське угруповання під назвою "Killnet" (інша назва "Легіон") 16 травня 2022 року оголосило кібервійну урядам десяти держав, які, на їх переконання, підтримують так званих "нацистів і русофобію". Відповідне звернення вони виклали на своєму Telegram-каналі. Пізніше хакери окремо уточнили, що кібервійна стосується таких країн, як США, Великобританія, Німеччина, Італія, Латвія, Румунія, Литва, Естонія, Польща та Україна. У вересні 2022 року хакери цієї групи вивели з ладу японський аналог "Дії", японську соціальну мережу "Mixi" та платіжний сервіс "JCB".У своїй оприлюдненій заяві хакерське угрупування "KillNet", яке пов'язують з рф, пригрозило Японії та порадило подумати, з ким воювати цій країні. За наслідками атаки, уряд Японії повідомив про проблеми з доступом до понад 20 веб-сайтів чотирьох державних міністерств, які постраждали від DDoS-атаки. Згодом цифрова агенція Японії повідомила про проблеми з авторизацією на адміністративному порталі e-Gov, проте причина складнощів не уточнювалася. За деякими даними, цей портал також був одним із жертв атаки "KillNet". Причинами активності "KillNet" щодо цілеспрямованих атак на Японію стала підтримка її урядом України, а також суперечки з Росією з приводу низки Курильських островів.

Влітку 2022 року корпорація Microsoft повідомила, що зірвала спроби хакерів, пов'язаних з військовою розвідкою рф, несанкціоновано проникнути в українські, європейські та американські мережеві об'єкти. Зловмисники позиціонують себе як угрупування "Strontium" (також називають "Fancy Bear" або "APT28") – команда хакерів, яка тісно пов'язана з російським агентством військової розвідки та відома потужними атаками на інформаційні системи урядових, військових і безпекових організацій. Вказана група хакерів використовувала 7 Інтернет-доменів з метою шпигування за державними органами та аналітичними центрами в ЄС та США, а також за українськими установами, зокрема й електронними ЗМІ. Отримавши дозвіл суду, корпорація Microsoft взяла під оперативний контроль ці Інтернет-домени, чим зменшила використання їх хакерами угрупування "Strontium" та отримала можливість завчасно

сповіщати про інциденти потенційних жертв. У компанії Microsoft вважають, що хакери групи “Strontium” намагалися встановити довгостроковий доступ до телекомунікаційних систем, забезпечити тактичну підтримку вторгнення та вивести наявну конфіденційну інформацію. Корпорація своєчасно повідомила уряд України про виявлену активність та результати вжитих заходів [8]. Компанія Microsoft виправила вразливість нульового дня у поштовому клієнті Outlook під ідентифікатором CVE-2023−23–397. Неполадка використовувалася при зломах сайтів 15-ти урядових, військових, енергетичних і транспортних організацій. Експлойти відбувалися з квітня по грудень 2022 року. З’ясовано, що до атак причетна група хакерів, яка тісно пов’язана з російськими спецслужбами. Фахівці відстежують хакерське угруповання під різними назвами: “APT28”, “STRONTIUM”, “Sednit”, “Sofacy” або “Fancy Bear”. Зловмисники можуть скористатися цією вразливістю, надіславши спеціально створений електронний лист, який спрацьовує автоматично, коли його обробляє клієнт Outlook. Під час підключення до віддаленого SMB-сервера від користувача надсилається повідомлення про узгодження NTLM (протоколу аутентифікації, який використовується в ОС Windows для перевірки автентичності користувачів), яке зловмисник може потім передати для перевірки автентичності в інших системах, що підтримують NTLM. Вразливість CVE-2023−23–397 впливає на всі підтримувані версії Microsoft Outlook для Windows, але не чинить шкоди версіям для Android, iOS або macOS. Оскільки онлайн-служби Outlook та Microsoft 365 не підтримують перевірку автентичності NTLM, вони невразливі для таких атак. Microsoft виправила несправність і закликає клієнтів негайно приєднатися до групи “Захищені користувачі” в Active Directory, а також заблокувати TCP-порт 445 – це допоможе мінімізувати подальші ризики експлойтів.

У січні 2023 року корпорація Microsoft виявила, що особливо активна російська команда хакерів, відома як “Sandworm”, випробовувала додаткові можливості програм-здирників, які можуть бути використані для руйнівних атак на організації за межами України, що виконують ключові функції в ланцюгах постачання. Атаки з використанням цих програм, як правило, передбачають проникнення хакерів на сервери організацій, шифрування даних і вимагання грошей в обмін на відновлення доступу. Програми-здирники також використовуються для прикриття більш зловмисної діяльності, зокрема знищення даних (так звані “чистильники”). Починаючи з січня 2022 року, корпорація Microsoft виявила щонайменше дев’ять різних “чистильників” і два типи програм-здирників, які використовувалися проти більш як 100 українських організацій. Також зросла кількість прихованих російських кібероперацій, спрямованих на компрометацію українських організацій на Заході. У країнах Америки та Європи, особливо в сусідніх з Україною, російські суб’єкти загроз намагаються отримати доступ до урядових і комерційних організацій, які беруть участь у підтримці України.

В умовах активної фази кібервійни, Україна на системній основі, продовжує виявляти факти спрямованих кібератак на державний сектор та критичну інфраструктуру. За даними Держспецзв’язку, протягом 2022 року було зареєстровано у 2,8 рази більше кіберінцидентів, ніж у 2021 році. А кількість подій інформаційної безпеки в категоріях “Шкідливий програмний код” та “Збір інформації зловмисником” зросла у 18,3 та 2,2 рази відповідно.

Оцінюючи Україну та вжиті нею заходи, світові експерти зазначають, що нашій країні вдалося уникнути найтяжчих наслідків та не допустити вразливостей за результатами масштабних російських кібератак. Це сталося завдяки тому, що українські кіберспеціалісти виявились найбільш ефективнішими, ніж російські. Нашій державі вдається ефективно та уважно відстежувати нові загрози та ризики. Також важливу роль

зіграло те, що більшість важливих українських ресурсів перенесені у “хмару”, тобто активно використовуються сучасні Хмарні технології. Таким чином, вітчизняний телеком-сектор продемонстрував свою стійкість та незламність перед обличчям російських кібератак та кіберзагроз.

Загалом механізми виявлення, блокування та протидії масштабному застосуванню шпигунського та шкідливого програмного забезпечення у мережах в умовах кібервійни включають такі фактори, як: технічний та людський.

Щодо технічного аспекту. Останнім часом стурбованість викликає динамічний розвиток штучного інтелекту (далі – ШІ) у світових масштабах. Значною загрозою для України залишається використання рф можливостей штучного інтелекту у зловмисних цілях. У сучасному цифровому світі кіберзагрози постійно розвиваються. Широке та динамічне використання ШІ в кібератаках стало однією зі значних подій останніх років. По мірі розвитку технологій ШІ зловмисники використовують їх для проведення більш витончених та ефективних атак. Навіть у НАТО визнали кібератаки з використанням ШІ критичною загрозою. ШІ можливо використовувати з метою злому мереж із використанням облікових даних та алгоритмів. Також у НАТО вважають, що атаки з використанням ШІ можуть здійснюватися не лише проти інфраструктури, а й для аналізу даних. Міжнародні дослідники ШІ заявили, що чат-бот ChatGPT навчився створювати програми-віруси, націлені на індивідуальні особливості та вразливості різних операційних систем. За оцінками експертів, такі системи як ChatGPT вже потенційно використовуються в кібердіяльності. Кіберзлочинці, навть ті що мають невеликий досвід програмування або зовсім його не мають, використовували ChatGPT з метою створення шкідливого програмного забезпечення та фішингових листів, які могли бути використані для проведення шпигунських дій, атак з вимогою виплати, спаму та інших шкідливих дій. Також можна знайти приклади того, як за допомогою ШІ російські хакери генерують коди шкідливих програм з потрібними властивостями під певні операційні системи, завдання та вразливості.

Основна відмінність оновлених можливостей ШІ в тім, що відтепер це можуть робити не тільки хакери, але й пересічні користувачі. Атаки, засновані на штучному інтелекті, викликають великі побоювання як з боку організацій, так і окремих осіб, оскільки такі кібератаки можуть обійти традиційні заходи безпеки та завдати значної шкоди. Тому дуже важливо застосовувати надійні заходи кіберзахисту.

Наразі кібератаки на основі ШІ можна умовно поділити на 5 основних видів.

Перший – вдосконалена постійна загроза (далі – APT). Це прихована загроза, за якою зазвичай стоїть держава або група, яка спонсорується державою, яка отримує несанкціонований доступ до комп’ютерної мережі і залишається непоміченою протягом тривалого періоду часу. APT-групи часто використовують ШІ, щоб уникнути виявлення та націлитися на свою жертву.

Друга – діпфейк-атаки. Для цих атак хакери використовують відео чи зображення, створені нейромережами, щоб видавати себе за реальних селебріті, проводити шахрайські кампанії чи дезінформацію.

Третій тип – використання шкідливого програмного забезпечення на базі ШІ, яке може працювати самостійно і адаптуватися до умов, що швидко змінюються. Також воно вміє уникати виявлення.

Четверте – фішинг, коли зловмисники можуть створювати електронні листи та повідомлення, призначені для того, щоб обманом змусити користувачів розкрити свої особисті дані.

П’ятий тип – DDoS-атаки, під час скоєння яких ШІ використовується з метою виявлення та використання вразливостей у мережі, що дозволяє кіберзлочинцю збільшити масштаб та вплив своєї атаки.

Також з позиції технічного ракурсу держава-агресор систематично впроваджує новітні розробки з метою поширення шкідливого програмного забезпечення у вітчизняному кіберпросторі. Наприклад, хакерське угрупування “Nodaria”, яке тісно пов’язане з рф, активно використовує нове шкідливе програмне забезпечення під час кібератак, спрямованих на Україну. Шкідливе програмне забезпечення, яке отримало назву “Graphiron”, є сучасною шпигунською розробкою. Це шкідливе програмне забезпечення поширювалося з метою збору широкого спектру інформації з інфікованих комп’ютерів, що включає: системну інформацію, облікові дані, знімки екрану та доступ до окремих файлів. Програма використовує імена файлів, призначені для маскування під легальні файли Microsoft Office, і схоже на інші інструменти TA471, такі як GraphSteel і GrimPlant. Раніше вони використовувалися як частина фішингової кампанії, спеціально націленої на українські державні органи, зокрема в січні 2022 року. Програму Graphiron розроблено для вилучення набагато більшої кількості даних, включаючи знімки екрана та приватні ключі SSH. Ця інформація може бути корисною сама по собі з точки зору завдань розвідки або її можна використовувати для глибшого проникнення в цільову організацію чи проведення інших деструктивних атак. Хакерське угрупування “Nodaria” уперше було помічене групою “CERT-UA” ще у січні 2022 року під час використання ними шкідливих програм “SaintBot” та “OutSteel” з метою фішингових атак на українські державні структури.

Також у 2022 році вітчизняними експертами було виявлено новий тип деструктивного шкідливого програмного забезпечення “Wiper”, який вражає комп’ютери та комп’ютерні системи в Україні. Це вже щонайменше третій штам сімейства “Wiper”, який вразив українські системи з початку російського вторгнення. Шкідливе програмне забезпечення, що отримало назву “CaddyWiper”, було виявлено фахівцями компанії ESET. За даними фахівців, “CaddyWiper” знищує дані користувача та інформацію про розділи з будь-яких накопичувачів, підключених до скомпрометованої системи. Опублікований приклад коду передбачає, що шкідлива програма пошкоджує файли на накопичувачі, перезаписуючи їх символами нульового байта, що робить їх невідновними. Раніше дослідники виявили два інших штами шкідливого програмного забезпечення “Wiper”, націленого на комп’ютери в Україні. Перший штам під назвою “HermeticWiper” був виявлений 23 лютого 2022 року, за день до того, як рф розпочала військове вторгнення в Україну. Версія “IsaacWiper” була розгорнута в Україні 24 лютого 2022 року. При цьому експерти припускають, що “IsaacWiper” і “HermeticWiper” перебували в розробці за декілька місяців до їх появи. Їхні перші зразки були виявлені ще у жовтні та грудні 2021 року.

Програми-вайпери мають деяку подібність із програмами-здирниками з погляду їхньої здатності отримувати доступ та змінювати файли в скомпрометованій системі. Але на відміну від програм-здирників, які шифрують дані на диску до моменту отримання викупу, програми-вайпери незворотньо видаляють дані з накопичувача і не дають змоги відновити їх. Таким чином, ціль цього типу шкідливого програмного забезпечення полягає виключно в тому, щоб завдати шкоди мішені, а не отримати будь-яку фінансову винагороду для зловмисника. У січні 2023 року дослідники компанії із забезпечення безпеки мобільних пристроїв “ThreatFabric” виявили нове шкідливе програмне забезпечення для Android під назвою “Hook”. Проникаючи в мобільний телефон або гаджет, цей вірус передає оператору призначені для користувача дані та

встановлює повний контроль над пристроєм. Додаток може переглядати та завантажувати повідомлення, контакти, історію пошуку і навіть листування з месенджерів. Головною ціллю “Hook” є банківські додатки, що належать фінансовим структурам та організаціям по всьому світу. За даними дослідників, “Hook” створила кіберзлочинна група “DukeEugene”. Вони також відповідальні за розробку інших небезпечних Android-вірусів, зокрема “BlackRock” і “ERMAC”.

Росіяни шукали та шукають вразливості та методи проникнення не тільки до грошей та персональних даних українських громадян, але і вигадують методики отримання доступу до державних систем та об’єктів критичної інфраструктури. На цьому фоні застосування шкідливого програмного забезпечення стає одним із найпоширеніших кримінальних правопорушень у сфері кібербезпеки. Їх використовують для комп’ютерного тероризму, майнингу криптовалюти, заволодіння персональною інформацією з електронних баз даних, порушення прав інтелектуальної власності, учинення шахрайства в електронних мережах тощо. У зв’язку з тим, що шкідливі програмні засоби набули широкого розповсюдження, треба знати і володіти способами їх уникнення. Превентивними способами захисту в цьому напрямі можуть бути: ретельна перевірка матеріалів, що користувач завантажує на свій девайс; використання електронних сертифікатів та безпечних протоколів передачі даних; регулярне тестування обладнання антивірусами на наявність шкідливого програмного забезпечення [9]. Ключові дії яких потрібно вжити, щоб знизити рівень шкоди, яку може завдати шкідливе програмне забезпечення – це забезпечити наявність актуальних резервних копій важливих файлів, за їх наявності можливо відновити свої дані ігноруючи вимоги зловмисників. Резервне копіювання є ефективним заходом зниження ризиків від впливу “ransomware”. Також необхідно перевіряти можливість відновлення даних із резервних копій.

Хмарні сервіси (*Cloud service*), що використовують синхронізацію (наприклад, Dropbox, OneDrive та SharePoint або Google Drive) за рекомендацією фахівців не слід використовувати як єдине середовище для збереження резервних копій. Недоліком даних систем є те, що вони можуть автоматично синхронізуватися відразу після ураження файлів, і тоді можливо втратити й резервні копії також. Можливо зменшити ймовірність розповсюдження шкідливого програмного забезпечення у мережі за допомогою:створення політик, що дозволить завантаження лише файлів тих типів, які мають надходити (наприклад заборонити отримання чи передачу EXE-файлів); блокування веб-сайтів, які є шкідливими; перевірки антивірусними програмами файлів, що викликають підозру, а в разі відсутності ліцензійного антивірусу рекомендується використовувати безкоштовний сервіс VirusTotal чи Cuckoosandbox; використання сигнатур для блокування відомого шкідливого коду. Зазвичай, вищеназвані функції формуються системами на кшталт мережевих екранів, а не пристроями користувачів. Наприклад:фільтрація пошти (у поєднанні зі фільтруванням спаму), яка може блокувати шкідливі повідомлення електронної пошти та видаляти підозрілі вкладення; використання засобів, які блокують відомі шкідливі веб-сайти за відповідними списками;використання засобів з функціями інформаційної безпеки, які можуть перевіряти вміст даних на предмет відомих зловмисних програм.

Також слід активно вживати превентивних заходів з метою запобігання шкідливому програмному забезпеченню. Необхідні кроки можуть бути різними для кожного типу пристроїв та операційних систем, але слід звернути увагу на такий метод захисту як централізоване керування пристроями підприємства для того, щоб: дозволяти встановлювати лише те програмне забезпечення, яким довіряє організація (як приклад використання AppLocker); дозволяти запускати програми лише з надійних джерел чи ті,

що мають відповідні сертифікати розробників; використання антивірусного програмного забезпечення з технологією евристичного аналізу та вчасне оновлення його бази сигнатур. Рекомендується не підключати флеш-пристої та зовнішні диски, а також не використовувати CD та DVD, якщо немає довіри щодо первинного джерела; вимкнення або обмеження використання макросів (використовуються в багатьох офісних продуктах, наприклад Microsoft Office, CorelDRAW, Notepad++).

Також українській кіберспільноті в умовах війни доцільно підтримувати налаштування та своєчасно оновлювати гаджети та мобільні пристрої, а саме: встановлювати оновлення безпеки, як тільки вони стануть доступними, щоб виправити недоліки, що використовуються на пристроях; увімкнути автоматичні оновлення для операційних систем, програм та мікропрограмного забезпечення, за можливості використовувати сучасні версії операційних систем та додатків, щоб скористатися найновішими функціями кібербезпеки. Обмежити вплив шкідливого програмного забезпечення стає можливим завдяки: використанню двофакторної аутентифікації; використанню програмних міжмережевих екранів (брандмауер) та штатних засобів захисту ОС від шкідливого програмного забезпечення; здійснювати регулярний перегляд прав користувачів, налаштовувати відповідні політики мережі, щоб використовувалися тільки лише необхідні порти та інтерфейси.

У випадку виявлення шкідливого програмного забезпечення та з метою збереження доказів несанкціонованого впливу необхідним є: зміна облікових даних, включаючи паролі (особливо для адміністраторів); відновлення даних з резервної копії; за необхідності перевстановлення операційної системи; оновлення та запуск антивірусного програмного забезпечення; відстеження мережевого трафіку на предмет підозрілої мережевої активності.

Враховуючи викладене, важливим питанням на державному рівні є посилення захисту від кібератак ворога та несанкціонованого доступу до електронних комунікаційних мереж, що передбачає удосконалення оперативно-технічного управління електронними комунікаційними мережами та відповідними послугами. Питання оперативно-технічного управління електронними комунікаційними мережами та послугами в умовах надзвичайного та воєнного стану, основні завдання Національного центру оперативно-технічного управління мережами телекомунікацій закріплені у статті 32 Закону України “Про електронні комунікації” [10]. Розуміючи ризики та загрози у цій площині, 30 січня 2023 року було прийнято розпорядження Національного центру оперативно-технічного управління (далі – НЦУ) при Держспецзв’язку “Про впровадження системи фільтрації фішингових доменів” № 67/850 [11], яке опубліковане на веб-сайті НЦУ до відома та виконання постачальниками електронних комунікаційних мереж та послуг – провайдерами DNS. Цим розпорядженням також було схвалено Регламент роботи системи фільтрації фішингових доменів.

На підставі цього розпорядження була створена централізована система автоматичного блокування Інтернет-ресурсів, що, за задумом авторів, надасть змогу збирати інформацію про користувача, який намагався зайти на заборонені сайти, автоматично зафіксувати та передати до відповідних уповноважених органів. До 2 березня 2023 року українські Інтернет-провайдери мали встановити систему блокування доступу до веб-ресурсів, яка кожні 15 хвилин автоматично завантажує на сервер провайдера з вказаного в розпорядженні ресурсу перелік Інтернет-адрес для автоматичного блокування. Інформація про користувача, який намагався зайти на “заборонені” ресурси, автоматично фіксується і передається до відповідних державних органів. І хоча система декларується для протидії фішингу, вона може бути використана

для блокування довільної кількості Інтернет-ресурсів. Таким чином, на державному рівні було запроваджено систему автоматичного блокування Інтернет-ресурсів.

З 2 березня 2023 року в Україні на виконання нормативних вимог провайдери відстежують тих, то відвідує заборонені сайти та запроваджені заходи щодо посилення боротьби з фішингом. Проте Інтернет-асоціація України з цього приводу продемонструвала своє занепокоєння та звернулася до уповноважених державних органів (РНБО, СБУ, ГУР МО) з вимогою анулювати вказане розпорядження та скасувати запровадження такої системи через те, що вона суперечить чинному законодавству України та шкодить її національним інтересам. На переконання представників Інтернет-асоціації України, дія розпорядження НЦУ поширюється абсолютно на усіх постачальників електронних комунікаційних мереж та послуг, встановлює для них додаткові обов'язки у відносинах, які не визначені та не регулюються Законом України "Про електронні комунікації" [10]. Дія розпорядження НЦУ, встановлені ним обов'язки поширюються на усіх без виключення постачальників електронних комунікаційних мереж та послуг, в той час, як багато з них взагалі не мають свого DNS-серверу. І хоча система декларується для протидії фішингу, вона, на переконання представників Інтернет-асоціації України, може бути використана для блокування довільної кількості Інтернет-ресурсів, що є значним порушенням прав користувачів. Таким чином, Інтернет-асоціація України закликає терміново скасувати розпорядження НЦУ № 67/850 від 30 січня 2023 року з метою опрацювання альтернативних шляхів протидії фішингу з прийнятим рівнем ризику, виходячи із кращих практик зарубіжного досвіду.

Слід вказати, що в Україні на виконання вказаного розпорядження НЦУ, Інтернет-провайдерів, які відмовляються блокувати російську пропаганду, почали виключати з Реєстру операторів, провайдерів телекомунікацій. Далі на компанію чекає застосування більш серйозних санкцій. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та послуг поштового зв'язку, прийняла рішення про виключення ТОВ "НЕТАСІСТ" та ТОВ "НЕТАССІСТ" з Реєстру операторів, провайдерів телекомунікацій через невиконання розпоряджень і вимог НЦУ під час воєнного стану, зокрема, щодо безпеки електронних комунікаційних мереж і послуг та блокування ворожих доменів в Україні [12].

Щодо людського аспекту. Людський фактор запобігання та протидії поширенню шпигунського та шкідливого програмного забезпечення передбачає фізичне затримання та кримінальне переслідування за результатами успішної реалізації спецоперацій відносно проросійськи налаштованих хакерів та кіберзлочинців, які навмисно поширюють його в мережах. У вересні 2022 року Служба безпеки України повідомила про нейтралізацію хакерського угруповання, яке діяло у Львові в інтересах країни-агресора. Викрадену конфіденційну інформацію зловмисники продавали через анонімну платформу "Даркнет", а гроші отримували на заборонені в Україні електронні платіжні системи "ЮMoney", "Qiwi" та "WebMoney". Таким чином, хакери продали орієнтовно 30 млн. акаунтів і одержали за це майже 14 млн. грн. За даними слідства, до складу угруповання входило декілька хакерів зі Львова. Також встановлено, що зламані акаунти використовували нібито від імені пересічних громадян з метою поширення дезінформації щодо стану суспільно-політичної ситуації в Україні та ЄС. Клієнтами злочинців були переважно прокремлівські пропагандисти. Саме вони використовували одержані установчі дані українських та іноземних громадян для поширення фейкових "новин" з фронту та створення панічних настроїв. Спеціалізоване комп'ютерне обладнання зловмисники встановили у своїх помешканнях. Зловмисники "проникали" до чужих акаунтів через шкідливе програмне забезпечення. Під час обшуків правоохоронці виявили жорсткі магнітні диски з

персональними даними громадян, комп'ютерну техніку, мобільні телефони, сім-карти та флеш-накопичувачі з доказами незаконної та протиправної діяльності [13].

У лютому 2023 року Службою безпеки України було викрито в столиці України злочинну схему продажу персональних даних українських громадян. Зловмисники створили спеціалізовану Інтернет-платформу і Телеграм-бот, в які зливали паспортні дані, номери телефонів і автомобілів, що належали мешканцям різних регіонів України. Для отримання доступу до електронних баз даних замовники купували "підписку" на відповідні Інтернет-ресурси. Ділки пропонували придбати "абонемент" на місяць вартістю до $200 США. З метою пошуку клієнтів використовували спеціально створені Телеграм-канали, а оплату отримували на криптогаманці. За оперативними даними, серед потенційних замовників Інтернет-послуг були представники російських спецслужб, які шукали конфіденційну інформацію про військовослужбовців Сил оборони. Під час обшуків за адресами проживання зловмисників виявлено комп'ютерне обладнання та інші речові докази скоєних злочинів [14].

Так, у березні 2023 року у містах Києва і Харкова вітчизняні правоохоронці реалізували міжнародну операцію щодо виявлення одного із членів хакерського злочинного угруповання, яке завдало європейським компаніям майже 40 млн. Євро збитків. Поліцейські служби Німеччини та України провели спільну операцію проти хакерів з угруповання "Double-Spider" ("Подвійний павук"), відповідальних за здійснення масштабних кібератак за допомогою програми-вимагача "DoppelPaymer", яке зашифровувало дані на комп'ютерній техніці. З 2020 року вони паралізовували діяльність переважно фінансових установ та організацій, підприємств критичної інфраструктури у різних країнах ЄС. У Нідерландах компанія, яка стала жертвою групи вимагачів, заплатила викуп у розмірі 27 BTC, що на той час становило еквівалент одного мільйона Євро. Інша потерпіла фінансова компанія заплатила викуп 250000 Євро. На даний час відомо про 37 потерпілих – європейських компаній, об'єктів критичної інфраструктури і промисловості. Загальна сума збитків становить майже 40 млн. Євро. Для відновлення доступу зловмисники вимагали викуп в криптовалюті. Під час розшукових дій правоохоронці провели обшуки на території декількох держав Європейського Союзу та України з метою виявлення активних членів хакерської групи, які використовували шкідливе програмне забезпечення. Загалом вдалося ідентифікувати 11 осіб, пов'язаних з цим хакерським угрупуванням, які проживають в Україні, Німеччині та Молдові, декілька з яких затримано. Слідчі дії здійснювалися Головним слідчим управлінням Національної поліції України за оперативного супроводу Управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції Нацполіції України [15].

Виходячи із вищевикладеного, в сучасних умовах проблематика посилення стану кібербезпеки набуває світових масштабів, особливо під час міжнародного протиборства на фоні російської військової агресії в Україні. Характеризуючи саме по собі кіберсуперництво, можна констатувати, що російські хакери та кіберзлочинці докладають значних й потужних зусиль з метою здобуття переваги й прагнуть перемоги на усіх фронтах в кіберпросторі. Проте результати їх дій не є однозначними. На цьому фоні держава-агресор активно поєднує кібернетичну та інформаційну складову у проведенні своїх інформаційно-психологічних спеціальних операцій, однак ці зусилля також залишаються неефективними.

2 березня 2023 року у США було оприлюднено нову національну стратегію кібербезпеки. Цей стратегічний документ чітко формулює завдання, вирішення яких надасть приватним особам, державним структурам та бізнесу можливість консолідовано діяти в цифровій сфері з мінімальними ризиками. Стратегія декларує необхідність

здійснити перебалансування відповідальності щодо посилення захисту кіберпростору, переклавши тягар забезпечення кібербезпеки з окремих осіб, малих підприємств і органів місцевого самоврядування на технологічні корпорації та компанії, які мають найбільші спроможності й найкращі рейтингові позиції. Перспективами розвитку цифрового технологічного прогресу вбачаються динамічні зміни та стимулювання розвитку американської ІТ-галузі на користь довгострокових інвестицій, дотримання балансу між захистом від нагальних загроз сьогодні та одночасним стратегічним плануванням й інвестуванням у стійке цифрове майбутнє. Стратегія визначає, що Уряд США повинен скоординовано використовувати всі наявні важелі та інструменти для захисту основ національної безпеки, громадської безпеки та загального економічного процвітання. Ця стратегія встановлює шляхи щодо ліквідації загроз і забезпечення гарантованого процвітаючого цифрового майбутнього. Стратегія спрямована на потужний захист інвестицій у відбудову американської критичної інфраструктури, розвиток сектору відновлювальної енергії та розвиток американських цифрових технологій та виробничої бази. США мають намір удосконалити власну цифрову екосистему, яка базується на таких ключових принципах, як: захищеність, стійкість, цінність діджиталізації. Стратегія побудована на п’яти основних засадах, серед яких пріоритетним є: захист критичної інфраструктури; ліквідація, запобігання та блокування будь-яких кіберзагроз; формування ринкових потужностей цифрової економіки, що гарантують кібербезпеку, інноваційний розвиток безпечних та стійких технологій й інфраструктури наступного покоління; розбудова міжнародного цифрового партнерства. Зауважимо, що Стратегія була розроблена після низки великих та потужних кібератак, включаючи напад на трубопровід ColonialPipeline у 2021 році й кіберзлам федеральних установ протягом 2019 – 2020 років [16].

Висновки.

Ворог використовує увесь наявний арсенал сил та засобів, які включають діяльність хакерів, кіберзлочинців та зловмисників з метою досягнення своїх амбітних злочинних цілей у кіберпросторі, використовуючи традиційні засоби ураження – віруси, трояни, програми-вимагачі, хробаки та інші. Хакери, які пов’язані з державою-агресором,можуть на перманентній основі готувати нову хвилю цілеспрямованих кібератак проти України, а також щодо установ та організацій інших країн, які надають допомогу нашій державі.

За допомогою шпигунського та шкідливого програмного забезпечення російські кібергрупи коригують свою діяльність з метою посилення руйнівного впливу та збору розвідувальної інформації про цивільні й військові об`єкти України та її партнерів. Це призводить до необхідності розробки та удосконалення на державному рівні механізмів виявлення, блокування та протидії застосуванню ворогом шпигунських та шкідливих програм на системній основі. Найпростішим способом запобігання є використання на усіх рівнях спеціалізованого програмно-апаратного забезпечення, що надає змогу підвищити рівень захисту мереж від зловмисних дій, а також допомагає ефективно та безпечно використовувати можливості сучасних мобільних пристроїв, гаджетів, комп’ютерів тощо. На нашу думку, медіаграмотність – саме та необхідна й обов’язкова навичка, яка може убезпечити від ймовірних та реальних негативних впливів, наслідків. З перших днів повномасштабного вторгнення українці проявили надзвичайну стійкість і виступили єдиним сучасним консолідованим інформаційним фронтом проти держави-агресора. Тому в час війни медіаграмотність необхідна – без жодних перебільшень – для захисту свого життя. Адже підступний ворог веде проти нас війну не лише на полі бою, він намагається вразити нас в інформаційному просторі з метою досягнення таких для нього завдань, як: поширення зневіри, зведення нанівець підтримки західних партнерів,

поширення страху та паніки, створення в кожного українця хибного враження, що війну програно. На цьому фоні, останнім часом ворог все частіше вдається до проведення інформаційно-психологічних спеціальних операцій.

Відтак, небезпека збільшення кількості серйозних кібератак у 2023 році залишається і навіть постійно динамічно зростає, що потребує посилення спроможностей відповідальних суб'єктів у рамках проведення та реалізації заходів забезпечення кібербезпеки на усіх рівнях. Вірогідно, що у 2023 році російські хакери можуть звернутися по допомогу у своїх злочинних цілях до активного використання програм ШІ під час проведення кібератак, залучаючи при цьому китайських та іранських фахівців та їхні напрацювання й розробки. Не виключається, що у майбутньому російські кіберзлочинці використовуватимуть саме ШІ для масштабування своїх атак, які включатимуть атаки об'єктів з відкритим кодом.

Виходячи із викладеного, для нашої держави залишається важливим пріоритетом: постійно превентивно та цілеспрямовано боротися з наслідками поширення шкідливого програмного забезпечення, переважно російського походження з метою мінімізації ймовірності інфікування комп'ютерних систем; виявляти та запобігати на системній основі поширенню шкідливого програмного забезпечення в структурах державного та приватного сектору(особливо щодо об'єктів критичної інфраструктури); максимально нівелювати негативний вплив шкідливого програмного забезпечення у вітчизняному сегменті кіберпростору, впроваджувати кращі практики зарубіжного інноваційного досвіду та сучасних напрацювань держав НАТО щодо посилення кіберзахисту.

Використаналітература

1. Войтович О.П., Вітюк В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. *Інформаційні технології та комп'ютерна інженерія.* 2013. № 3. С. 4-9.

2. Козачок В.А., Рой А.А., Бурячок Л.В. Технології протидії шкідливим програмам та завідом фальшивому програмному забезпеченню. *Сучасний захист інформації.* 2017. № 2 (30). С. 30-34.

3. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. *Інформація і право*. № 4(31)/2019. С. 98-106.

4. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності *Інформація і право*. № 1(18)/2018. С. 127-132.

5. Пеньков В.І., Штонда Р.М., Гук О.М., Мальцева І.Р., Черниш Ю.О. Методи та засоби протидії шкідливому програмному забезпеченню. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2017. № 2 (29). С. 58-64.

6. Russia's Cyber Tactics: Lessons Learned 2022: аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни росії проти України. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53466

7. Google виявив п'ять хакерських угруповань пов'язаних з рф, які атакують країни НАТО та Україну. URL: https://zmina.info/news/google-vyyavyv-pyat-hakerskyh-ugrupovan-povyazanyh-z-rf-yaki-atakuyut-krayiny-nato-ta-ukrayinu

8. Disrupting cyberattacks targeting Ukraine URL: https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia

9. Юхно О.О., Заворіна М.А. Шкідливий програмний засіб як інструмент вчинення кримінального правопорушення: матеріали І міжнар. наук.-практ. конференції *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення*, м. Дніпро, 17 черв. 2021 р. Дніпро: ВНПЗ "Дніпровський гуманітарний університет", 2021. С. 228-229.

10. Про електронні комунікації: Закон України від 16.12.20 р. № 1089 URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

11. Про впровадження системи фільтрації фішингових доменів: розпорядження Національного центру оперативно-технічного управління мережами телекомунікацій (НЦУ) від 30.01.23 р. № 67/580. URL: https://nkrzi.gov.ua/images/news/11/2580/67_30012023.pdf

12. Провайдерів, які відмовляються блокувати пропаганду Росії, виключають із реєстру, – Держспецзв'язку. URL: https://ukranews.com/ua/news/845667-provajderiv-yaki-vidmovlyayutsya-blokuvaty-propagandu-rosiyi-vyklyuchayut-iz-reyestru-derzhspetszv

13. СБУ викрила хакерів, які "зламали" майже 30 млн. акаунтів в Україні та ЄС та продали їх Росії. URL: https://ms.detector.media/kiberbezpeka/post/30310/2022-09-23-sbu-vykryla-khakeriv-yaki-zlamaly-mayzhe-30-mln-akauntiv-v-ukraini-ta-ies-ta-prodaly-ikh-rosii

14. СБУ викрила ділків, які продавали персональні дані українців громадянам рф. URL: URL: https://ssu.gov.ua/novyny/sbu-vykryla-dilkiv-yaki-prodavaly-personalni-dani-ukraintsiv-hrom adi anam-rf

15. В Україні викрили члена міжнародної хакерської групи. *Закон і бізнес*. – (8.03.2023 р). URL: https://zib.com.ua/ua/155176.html

16. National Cybersecurity Strategy. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

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