УДК 342.951

ФЕДІЄНКО О.П., здобувач наукового ступеня.
ORCID: https://orcid.org/0009-0008-5383-3504.

ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ ДЕРЖАВОЮ-АГРЕСОРОМ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

DOI...

Анотація. *Визначені тенденції використання шкідливого програмного забезпечення російськими хакерами та кіберзлочинцями на замовлення спецслужб рф. Окреслено масштаби та наслідки поширення шкідливого програмного забезпечення у світових вимірах. Деталізовано загрози та ризики, пов'язані із кібератаками та поширенням шкідливого програмного забезпечення. Акцентовано увагу на використанні кіберзлочинцями мережі TOR в сучасних умовах. Узагальнено завдання діяльності спецслужб рф в умовах кібервійни, форми та методи проведення атак з використанням шкідливого програмного забезпечення. Актуалізовано методологію поширення шкідливого програмного забезпечення через такі механізми як фінансове шахрайство та фішинг. Розкрито особливості поширення шкідливого програмного забезпечення російського походження. Висвітлено здобутки щодо набуття Україною членства в структурах НАТО з питань співробітництва в галузі кіберзахисту. Визначено подальші шляхи удосконалення чинного законодавства у питаннях протидії шкідливому програмному забезпеченню, зокрема фішингу.*

Ключові слова: *шкідливе програмне забезпечення, кібербезпека, кібератака, фішинг, кібершахрайство, спецслужба, національна безпека, державні інтереси, кібершпигунство, хакери, кіберзлочинці, експлойт, кібердомен.*

Summary. *The trends in the use of malware by the russian hackers and cybercriminals commissioned by the special services of the Russian Federation have been determined. The scope and consequences of the spread of malware on a global scale are outlined. The threats and risks associated with cyber-attacks and the spread of malicious software are detailed. The attention is focused on the use of the TOR network by cybercriminals in modern conditions. The tasks of the special services of the Russian Federation in the conditions of cyber warfare, the forms and methods of conducting attacks using malicious software are summarized. The methodology of spreading malicious software through such mechanisms as financial fraud and phishing has been updated. The peculiarities of the distribution of malicious software of Russian origin have been revealed. The achievements related to Ukraine's acquisition of membership in the NATO structure on cooperation in the field of cyber defense are highlighted. The further directions of improving the current legislation in the matter of combating malware, in particular phishing have been determined.*

Keywords*: malware, cyber security, cyber attack, phishing, cyber fraud, special service, national security, state interests, cyberespionage, hackers, cybercriminals, exploit, cyber domain.*

Постановка проблеми. Перманентний характер загрозливих тенденцій використання шкідливого програмного забезпечення (далі – ШПЗ) російськими хакерами та кіберзлочинцями на замовлення федеральних спецслужб рф демонструє високий рівень. На рф працює ціла армія хакерів, мішенями кібератак яких стають інформаційні ресурси органів державної влади та місцевого самоврядування, критична інформаційна інфраструктура, складові сектору безпеки та оборони тощо. Типовою методологією кібератак є збір інформації OSINT, використання шкідливого програмного

коду, нахабне втручання в ту чи іншу державну цифрову інформаційну інфраструктуру, виведення з ладу державних та приватних електронних комунікацій. На цьому фоні, розуміючи ризики та виклики, наша держава, попри війну, активно розпочала здійснення оцифрування багатьох державних сервісів з метою суцільної цифровізації державних послуг, переведення їх в режим онлайн, що, у свою чергу, стало ефективним інструментом протидії російській агресії у кібердомені. Останні події переконливо довели важливість та необхідність посилення захисту державних інформаційних систем, конфіденційних та персональних даних від несанкціонованого доступу, доцільності адекватного реагування на застосування ШПЗ, запровадження інноваційних рішень та адаптацію до динамічно мінливого ландшафту кіберзагроз. Саме в таких умовах Україна продовжує героїчно та відважно боронити свої території і тримати оборону на кіберфронті, який працює у режимі 24/7. Тому розгляд проблемних питань щодо ШПЗ на замовлення спецслужб рф вмотивованими хакерами й зловмисниками на шкоду державним інтересам в умовах війни є своєчасним та необхідним.

Результати аналізу наукових публікацій. Технічний аспект виявлення та блокування ШПЗ висвітлювали: О. Волков [5], І. Жульковська [6], С. Лисенко [8]. ШПЗ у форматі реальної загрози кібербезпеці держави розглядали: В. Бойко [3], М. Василенко [4] та інші. Пошук оптимальних шляхів удосконалення методології боротьби з комп'ютерними вірусами та ШПЗ досліджували: Н. Антоненко [1], Л. Поліщук [9], Д. Ричка [11]. Особливості поширення ШПЗ спецслужбами рф, сучасні тренди виявлення та протидії їхньому застосуванню вивчали у своїх наукових працях: І. Білан [2], О. Поляков [10] тощо. Проте проблемні питання використання та поширення державою-агресором ШПЗ на шкоду державним інтересам в умовах кібервійни жоден із вказаних фахівців ретельно не досліджував, що засвідчує актуальність теми цієї наукової статті.

Метою статті є висвітлення загрозливих тенденцій використання ШПЗ хакерами та кіберзлочинцями на замовлення федеральних спецслужб держави-агресора, визначення подальших шляхів удосконалення чинного законодавства з метою запровадження ефективного механізму запобігання поширенню шкідливих програм, зокрема фішингу.

Виклад основного матеріалу. Загальновідомо, що тематика використання ШПЗ існує тривалий час, не одне десятиріччя. Війна в Україні викликала масштабування зростання комп'ютерних атак у всьому світі. Чимало хакерів, у тому числі переважно російських, використують свої напрацювання, розробки та можливості з метою поширення шкідливих програм, посягаючи на державні інтереси в інформаційній та кібернетичній сферах, практикуючи крадіжки конфіденційних даних користувачів тощо. Тобто актуальна загроза сучасності – розробка зловмисниками та хакерами нових зразків ШПЗ та постійне його удосконалення.

Нагадаємо, що у 2019 році ШПЗ під назвою "Joker" уразило мільйони пристроїв по всьому світу. "Joker" міг викрадати особисту інформацію користувачів, включаючи їхні паролі, номери кредитних карток та інші конфіденційні дані. Світовий лідер у галузі інформаційної безпеки компанія "ESET" повідомила про появу нового ШПЗ під назвою "AceCryptor", яке активно використовується з метою шифрування. Загалом, ця загроза поширюється у всьому світі з 2016 року, при цьому багато зловмисників використовують її для розповсюдження власних шкідливих програм. Протягом 2021 та 2022 років було зафіксовано понад 240 тис. випадків поширення цього ШПЗ, що становить понад 10 тис. щомісяця. Чимало зловмисників використовують цей шифрувальник для уникнення виявлення технічними безпековими рішеннями. Зокрема, загроза "AceCryptor" застосовувала численні способи обходу свого виявлення протягом останніх років. Використання групами кіберзлочинців "AceCryptor" поширюється різними способами.

Переважно ці загрози розповсюджувалися через шкідливі інсталятори програмного забезпечення або через спам-листи із небезпечними вкладеннями.

У травні 2023 року експертами було виявлено ще одне ШПЗ для Android під назвою "Guerrilla", яке інфікувало мільйони пристроїв по всьому світу. Це ШПЗ викрадає особисту інформацію користувачів, включаючи їхні паролі, номери кредитних карток та інші персональні дані. "Guerrilla" може отримати доступ і викрасти дані з будь-якої програми на пристрої користувача. Вказане ШПЗ є особливо небезпечним, оскільки здатне інфікувати пристрої, навіть якщо на них встановлені найновіші оновлення систем безпеки. Це пов'язано з тим, що "Guerrilla" інфікує пристрої не через програми, а шляхом модифікації ROM пристрою. Вважається, що "Guerrilla" була створена групою кіберзлочинців, які є відомими авторами й розробниками складного ШПЗ. Експерти вважають, що ця група діє вже кілька років і базується в Китаї. Виявлення ШПЗ "Guerrilla" є нагадуванням про те, що пристрої Android все ще залишаються досить вразливими до атак з використанням шкідливих програм.

Власник Facebook, компанія Meta, повідомила, що виявила постачальників шкідливого програмного софту, які використовують інтерес громадськості до штучного інтелекту ChatGPT, щоб заманити користувачів до завантаження шкідливих програм і розширень для браузерів. Зазначається, що з березня по травень 2023 року компанія Meta виявила близько 10 сімейств шкідливих програм і понад 1 тис. шкідливих посилань, які рекламувалися як інструменти з популярним чат-ботом на основі штучного інтелекту. У деяких випадках ШПЗ надавало робочу функціональність ChatGPT разом із шкідливими файлами. Таким чином, дедалі активніше штучний інтелект ChatGPT використовується задля створення вірусів, протягом декілька тижнів після свого запуску. Можливості штучного інтелекту ChatGPT ймовірно є новим інструментом для учасників Dark Web та середовища кіберзлочинців з метою його подальшого використання для створення шкідливого програмного коду.

Тільки у 2022 році було виявлено понад 30 млн. нових зразків ШПЗ в міру постійної еволюції кіберзагроз. Це означає, що хакери та зловмисники у середньому щоденно створювали понад 316 тис. шкідливих програм. За таких умов можна констатувати, що спостерігається загрозлива світова тенденція збільшення випадків та масштабів поширення ШПЗ, його постійне удосконалення і використання під час скоєння кібератак. На цьому фоні питання протидії загрозам у сфері кібербезпеки займає провідне місце у системі національної безпеки України. Особливої актуальності проблема кібербезпеки набула за сучасних обставин, що повністю формується під впливом тривалої гібридної війни та відкритого воєнного вторгнення рф на територію нашої держави. Такий стан національної безпеки потребує адекватного підходу до вирішення проблем безпеки, зокрема і щодо об'єктивного розуміння стану кібербезпеки в Україні та реалізації відповідної державної політики, спрямованої на ефективну протидію загрозам у сфері кібербезпеки [7, с. 119].

Наша держава зазнає кібератак із використанням ШПЗ різної потужності, починаючи ще з 2014 року. Війна в Україні стала своєрідним каталізатором глобального зростання кількості кібератак за допомогою ШПЗ. Рф залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна проактивність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [12].

Кібератаки та ШПЗ – це не міфи цифрового світу, а наша сучасна реальність. Дії російських зловмисників та хакерів від крадіжки конфіденційних даних для проведення т.зв "референдумів" на тимчасово окупованих територіях України до порушення штатної роботи цілих об'єктів державної інфраструктури спрямовані на заподіяння та масштабування шкоди державним інтересам та національній безпеці. ШПЗ – це програми, які спеціально розробляються з метою ушкодження комп'ютерної техніки, заподіяння шкоди комп'ютерній системі або мережі її використання, для протизаконних цілей без відома користувача або з метою крадіжки даних. Атаки шкідливих програм можуть мати різні форми, включаючи віруси, хробаків, шпигунські програми, рекламне ПЗ та програми-викрадачі. Ці атаки можуть бути ініційовані за допомогою різних засобів, таких як вкладення електронної пошти, завантаження з шкідливих веб-сайтів і уразливості програмного забезпечення.

До загальнопоширеного ШПЗ (*malware*) відносять будь-яке програмне забезпечення, яке несанкціоновано проникає в комп'ютерну техніку або до перефірійних пристроїв. Кінцевою метою поширення шкідливих програм може бути викрадання певної інформації, у тому числі й персональних даних певного користувача, ураження комп'ютерів вірусами, примусове взяття управління над певною кількістю комп'ютерів для запуску DDos-атак, спрямованих проти інших мереж тощо. ШПЗ – це програма або код, яка, проникнувши в комп'ютер, може завдати істотної шкоди. Іноді це означає – вивести систему з ладу, іноді – перехопити контроль чи оволодіти певною інформацією.

Без перебільшення, ШПЗ очолює рейтинги кібератак. Воно може діяти за декількома напрямками: забороняти доступ до мережі, "красти" інформацію з жорсткого диска та порушувати чи виводити з ладу систему. ШПЗ може бути у вигляді шпигунських програм, які збирають інформацію для подальшого викупу. Можуть бути задіяні спеціально розроблені програми-вимагачі. Вони шифрують дані користувача і вимагають викуп (зокрема у криптовалюті) за їхнє розшифрування.

Атаки з використанням шкідливих програм можуть набувати різних форм та поширюватися через віруси, трояни, хробаки, шпигунські програми, рекламне ПЗ та програми-викрадачі. Ці атаки можуть бути ініційовані за допомогою різних засобів, таких як вкладення електронної пошти, завантаження з шкідливих веб-сайтів і уразливості програмного забезпечення. Так, автори зловмисних програм іноді поєднують особливості різних форм ШПЗ, щоб зробити атаку більш потужною – наприклад, використання викупного програмного забезпечення як відволікання для знищення доказів нападу троянів. ШПЗ часто охоплює декілька категорій. Наприклад, програма може одночасно містити кейлогер, збирати паролі і бути хробаком для розсилки спаму. Одночасно зловмисники розробляють ШПЗ, щоб мати постійний бекдор-доступ до пристроїв державних структур та приватних компаній, який важко виявити. Тоді вони можуть дистанційно керувати пристроями та використовувати його для викрадення даних, дослідження локальної мережі або надсилання спаму із інфікованого пристрою. Інфікування є досить поширеним явищем і може негативно вплинути на мережу через крадіжку даних і паролів, уповільнення роботи систем і повне видалення файлів. Обладнання, інфіковане ШПЗ, часто стає непридатним для подальшого використання, що призводить до значних економічних витрат на його заміну.

Враховуючи швидкість передачі даних, потенційні можливості хакерів та кіберзлочинців постійно збільшуються. Одним із найбільш поширюваних програмних засобів, які маскують звернення кіберзлочинців до доменів мережі Інтернет є мережа TOR – це скорочення від англійської The Onion Router, ("ретранслятор") що відноситься до декількох шарів шифрування, які використовуються для захисту конфіденційності.

Основна функція TOR полягає у тому, що він приховує сліди в Інтернеті, дозволяючи переглядати веб-сторінки та завантажувати їх анонімно. Tor не є службою VPN або браузером зі вбудованою VPN. Хоча як TOR, так і VPN дозволяють здійснювати приватний веб-перегляд, це досить різні технології. TOR був спочатку розроблений військово-морським флотом США для захисту американських комунікацій під час розвідувальних операцій. Анонімізація трафіку забезпечується за рахунок використання розподіленої мережі серверів на рівні onion-маршрутизаторів, що гарантує повне маскування вихідних з'єднань, а також захист аналізу трафіку, забезпечуючи практично повну конфіденційність дій у мережі Інтернет. Також 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. 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. Як це ні парадоксально, браузер TOR визнано нелегальним у країнах з авторитарними режимами, в яких громадянам заборонено читати та спілкуватися анонімно. Наприклад, у КНР трафік TOR блокується всередині країни. Такі держави, як Саудівська Аравія та Іран, працюють над тим, щоб категорично заборонити громадянам мати можливість використовувати мережу TOR.

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 ШПЗ "WhisperGate", цілями якої виступають український державний та приватний сектор з метою організації крадіжок службової та конфіденційної інформації. Зловмисники націлені, у першу чергу на Україну, але також періодично атакують країни-члени НАТО в Північній Америці та Європі. Вказана хакерська група TA471 тісно пов'язана із зловмисним програмним забезпеченням "WhisperGate", на системній основі поширюють інше зловмисне програмне забезпечення для видалення даних. Це програмне забезпечення маскується під програми-вимагачі, але робить цільові пристрої повністю непрацездатними та нездатними відновлювати файли, навіть якщо виплачується викуп [2, с. 148].

Спецслужби рф, на постійній основі, займаються шпигунством в мережі Інтернет, збирають приватну та публічну інформацію, зламують комп'ютерні системи та мережі інших держав, блокують штатну роботу критичної інфраструктури. 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. Також спецслужби рф та хакери використовують ШПЗ з метою викрадення службової інформації в органах державної влади та місцевого самоврядування, ставлять за мету максимальне блокування штатного режиму роботи та виведення з ладу об'єктів критичної інфраструктури. Нещодавно дослідники виявили ШПЗ під назвою "CosmicEnergy", яке "кремль" використовує для навчання своїх хакерів. "CosmicEnergy" – програмне забезпечення, яке має за мету спричинення перебоїв в електропостачанні, небезпечний софт, що може вірогідно використовуватися у російських навчаннях, в тому числі, для атак на українську енергоінфраструктуру. "CosmicEnergy" є останнім

прикладом спеціалізованого ШПЗ, здатного спричиняти кіберфізичні впливи, які рідко виявляються. Унікальність "CosmicEnergy" полягає в тому, що воно є інструментом для навчань з метою скоєння цілеспрямованих перебоїв в електропостачанні.

Досить часто російські кіберзлочинці з метою досягнення своїх амбітних цілей вдаються до "атак нульового дня", які використовують раніше невідомі вразливості в системах кібербезпеки на макрорівні. Особливу увагу російські хакери приділяють перифірійним мережевим пристроям, таким як брандмауери та маршрутизатори. Атаки на ці системи стали особливо привабливими, оскільки програмне забезпечення для виявлення уразливостей кінцевих точок не охоплює ці пристрої та не забезпечує високий рівень захисту. Кібератака "нульового дня" є особливо небезпечною, оскільки зловмисник часто єдиний, хто знає про наявну вразливість. Він може вирішити скористатися цією перевагою негайно, але він також може зберегти її до більш вигідного моменту з метою подальшого перспективного використання. Кібератаки "нульового дня" завжди були прерогативою хакерів, які підтримуються державою, зокрема рф. Причиною цього є складність та досить велика вартість отримання доступу до уразливостей. Також відзначається збільшення кількості та швидкості реалізації загроз: від моменту появи відомостей про загрози, наприклад, публікації відомостей про уразливості, до її практичної реалізації проходить усього декілька годин.

Російські хакери використовують нові розробки ШПЗ для кібератак не тільки на державний сектор, але й на комерційні приватні структури. В жовтні 2022 року компанії України та Польщі були атаковані програмою-вимагачем "Prestige", яку експерти пов'язують із "кремлем". Хакери активізували комп'ютерний вірус 11 жовтня 2022 року, тобто наступного дня після масованого обстрілу України російськими військами. Жертви зіткнулися зі ШПЗ з різницею на годину, а їх список збігається з постраждалими від програмного забезпечення "FoxBlade" (також відомого як "HermeticWiper") та інших атак, які пов'язують із рф. Програма отримувала доступ до облікових записів користувачів, потім шифрувала файли, й додавала розширення "enc" і вимагала викуп в обмін на інструмент для розшифровки. Компанія Microsoft виділила декілька особливостей вірусу "Prestige", який раніше не траплявся експертам із кібербезпеки. Цей вірус використовує бібліотеку CryptoPP C++ для шифрування AES кожного відповідного файлу. У процесі шифрування одна версія програми-здирника використовує наступний жорстко запрограмований відкритий ключ RSA X509 (кожна версія "Prestige" може мати унікальний відкритий ключ). Це ШПЗ також видаляє резервні копії файлів, щоб їх неможливо було зупинити за допомогою функції відновлення системи.

Російські хакери, які повсякденно керуються федеральними спецслужбами рф, активно поширюють шкідливі файли через механізми та за допомогою безкоштовного доступу на торент-трекерах. Зокрема, якщо встановити такі файли на комп'ютер, зловмисники отримують доступ до вмісту комп'ютера й довгий час залишаються непомітними. Хакери використовують троянські програми, які мають на меті скопіювати паролі з різних сервісів та дізнатися певну інформацію. За інформацією Держспецзв'язку, системні адміністратори досить часто використовують неліцензійне програмне забезпечення, яке поширюється за допомогою торент-трекерів в установах та компаніях різних форм власності. Таким чином, встановлюючи неліцензійне програмне забезпечення з неофіційних джерел, торентів, користувачі перебувають у зоні підвищеного ризику. Тобто, жертвою хакерів можуть стати користувачі, які встановлюють неліцензійне програмне забезпечення з неофіційних джерел або торентів. 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.

Світ кібербезпеки постійно змінюється і майже щодня з'являються нові загрози. За результатами порушення вимог кібербезпеки настають шалені збитки як для державного, так і приватного секторів. Середня оцінка шкоди від витоку даних, наприклад у США становить $9,4 млн. США, а фішингові атаки викрадають приблизно $17700 США за хвилину. За таких умов, актуальною методикою поширення ШПЗ залишаються кібершахрайство та фішинг.

Російські зловмисники дедалі активніше використовують схеми кібершахрайства у своїх злочинних цілях. З початку повномасштабного вторгнення рф в Україну значно змінився патерн кібершахрайства. Майже дві третини компаній, які здійснюють шахрайські операції в Україні, належать державі-агресору. Сума збитків банків, торговців, клієнтів від незаконних дій з платіжними картками тільки за 2022 рік становила 481 млн. гривень, що на 46 % більше, аніж у 2021 році. Кількість незаконних дій з платіжними картками, за якими були понесені збитки, зросла торік на 8 %. Для оцінки рівня шахрайства з платіжними картками, зазвичай, аналізують не просто суму збитків, а порівнюють її із загальною сумою усіх видаткових операцій з платіжними картками. Щодня в Україні за посиланнями на шахрайські сайти переходять в середньому 10000 – 15000 громадян. Застосовуючи шкідливі ресурси, зловмисники та хакери намагаються ошукати громадян та отримати доступ до їхніх фінансових даних. Такі сайти в основному стилізовані під урядові портали, Дію, Є-Допомогу, під сайти українських банків, міжнародних організацій та відомих платіжних сервісів. Користувач, не усвідомлюючи, що це фейковий сайт, залишає на ньому інформацію, яку не слід розголошувати (наприклад, CVV-код, пін-код, логін та пароль для входу в Інтернет-банкінг, тощо). Після цього зловмисники просто крадуть її гроші з рахунків, або ж психологічно тиснуть на людину, вимагаючи здійснити платіж на користь шахраїв тощо.

Технології розвиваються дуже швидко, одночасно їх використовують також й шахраї. На цьому фоні зростає популярність злочинів з використанням ID-верифікації, а також дипфейків. Здебільшого клієнти здійснюють операції на смартфонах, використовуючи методи віддаленої ідентифікації, чим і користуються злочинці.

15 лютого 2023 року Національний координаційний центр кібербезпеки (НКЦК) при РНБО України спільно з Національним банком анонсували запуск автоматичної централізованої системи Protective DNS, що має протидіяти кібершахрайству у фінансовому секторі. Ще наприкінці 2022 року її успішно протестували. До цієї 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. Тільки за перший місяць роботи проекту було зафіксовано понад 120 тисяч унікальних переходів на сторінку, що у режимі реального часу попереджає про загрозу крадіжки облікових даних. Адже десятки зловмисних груп, які проводять фішингові кампанії проти українських громадян координуються російськими злочинцями під прикриттям федеральних спецслужб рф. Внаслідок цього кошти, які втрачають українці, використовуються для підтримки країни-терориста, а кількість фішингових атак постійно зростає через повномасштабне вторгнення рф в Україну, що потребує вжиття ефективних превентивних заходів [13].

Фішинг – це вид Інтернет-шахрайства, який полягає в крадіжці конфіденційних даних користувачів. Фішинг являє собою найпростіший спосіб кібератаки, який є одним із найнебезпечніших і у той же самий час ефективним. На відміну від інших загроз у

мережі Інтернет, фішинг не вимагає наявності глибоких знань та навичок. Зловмисники намагаються отримати доступ до персональних даних користувачів – номерів телефонів, номерів та кодів банківських карт, логінів та паролів електронної пошти та облікових записів в соціальних мережах тощо. 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, аби замаскуватися. Головна зброя фішингу – листи. Одна неправильна літера чи навіть крапка має насторожити користувача, стати сигналом 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 їх грошей.

У 2022 році НБУ виявив більше 4500 таких фішингових ресурсів. Водночас, у першому кварталі 2023 року вже виявлено більше 11 тис. подібних шахрайських доменів. У середньому щодня виявляється більше 100 таких шахрайських ресурсів. Операторами цих шахрайств здебільшого є угрупування з рф. Приблизно дві третини з виявлених сайтів є фішинговими (68 %), які походять саме з рф. На цьому фоні все ще однією із ефективних технік, яку використовують російські хакери для скоєння атак залишається саме фішинг [14]. Саме фішингові атаки – найпоширена проблема мережевої безпеки. Фішинг – один з найпоширеніших способів кібератак, які використовує рф. У той час як фільтри електронної пошти основних державних служб добре справляються з відсіюванням підробок від реальних повідомлень, все ж таки потрібно бути обережним і мати власні засоби захисту. Оператори та провайдери застерігають користувачів під час роботи з будь-якими зовнішніми спробами отримати конфіденційну чи особисту інформацію, що вимагає на постійній основі підтвердження за допомогою інших засобів зв'язку з метою з'ясування факту того, що відправник та запит є офіційними.

Виявляти фішингові повідомлення електронної пошти є технічно проблематичним. З метою захисту від фішингових листів корисною є система обслуговування електронної пошти з вбудованими розширеними функціями безпеки. Така система електронної пошти просканує посилання та визначить, безпечне воно чи ні, перш ніж перенаправити користувача на веб-сайт, та заблокує доступ із попередженням для користувача, якщо це відоме шкідливе посилання. Так само функція безпечного вкладення спочатку сканує вкладення в електронному листі, і якщо шкідливість програми підтверджується, вкладення буде замінено з повідомленням для користувача.

Для ураження веб-сайтів, що працюють на основі баз даних, російськими хакерами використовуються SQL-ін'єкційні атаки чи т.зв. "брутфорс". Брутфорс – це методика вгадування паролів, облікових записів для входу в систему, ключів шифрування та іншої інформації. Основна мета брутфорсу – отримання несанкціонованого доступу до баз даних, систем або мереж. Брутфорс-атаки зазвичай здійснюються ботами, які створюють великі армії інфікованих комп'ютерів у всьому світі, відомі як ботнети. Зловмисники використовують бот-мережі для багатьох спроб входу в облікові записи, використовуючи "довгий рядок" або "словник" у якості паролів. Брутфорс-атаки існують стільки, скільки й паролі, а сприятливим фактором для них став перехід користувачів на віддалену роботу. Існують такі види брутфорс-атак: проста атака методом підбору; атака за "словником", зворотня атака грубої сили; гібридна атака грубої сили; перевірка паролів, використання ботнетів тощо. В основі методу – використання шкідливого SQL коду для маніпуляцій з базою даних на сервері з метою отримати доступ до інформації, яка мала би залишатися прихованою. Результативна

брутфорс-атака може мати наслідком отримання хакерами та зловмисниками паролів, та особистої інформації, надає можливості виконувати адміністративні операції, відновлювати зміст файлів та навіть керувати операційною системою. Щоб запобігти можливості підбору паролів необхідно використовувати двофакторну авторизацію (логін-пароль + смс) або обмежити доступ з певних IP-адрес.

Значну небезпеку становлять і відкриті Wi-Fi мережі. Ненадійні паролі зазвичай стають причиною потужних хакерських атак. Після того як зловмисник підключиться до мережі, після проникнення він отримує 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, атака полягає у тому, що зловмисник може впровадити шкідливий код “JavaScript” жертві в незашифрованих HTTP-з’єднаннях з метою використання вразливостей у браузері жертви.

Згідно із річним звітом компанії Microsoft, у 2022 році кількість кібератак зросла у 3,5 рази, порівнюючи з 2021 роком. На фінансовий сектор України припадає 5 % усіх кібератак, на IT-галузь – майже 10 %. У другій половині 2022 року російські хакери змінили тактику – вони не атакують безпосередньо організації та установи за допомогою фішингу, а впроваджують новий підхід – використовують технічні уразливості сервісів, які надають послуги операторам критичної інформаційної інфраструктури. Запобігти цьому можливо завдяки шифруванню конфіденційних даних, створенню безпечного коду, відповідної архітектури та аутентифікації.

Проблема протидії ШПЗ залишається досить гострою, незважаючи на появу більш ефективних механізмів його виявлення, аналізу, оновлення баз його описів і правил виявлення [15, с. 30]. На жаль, 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 вітчизняних підприємств ВПК, органів виконавчої влади, об’єктів критичної інфраструктури тощо.

Останнім часом існують локальні випадки виявлення ШПЗ, що потребує прискіпливої уваги з боку правоохоронців. У травні 2023 року кіберполіцейські викрили мешканця м. Чернівці, який розробляв та збував ШПЗ. Фігурант власноруч розробив програму за типом “Obfuscated Web Backdoor” з метою шифрування програмного коду та модифікованого ШПЗ для віддаленого контролю над веб-ресурсами. Таким чином, його розробка дозволяла приховати ШПЗ на ураженому ресурсі та залишати контроль над ним непомітним для власника. Шкідливу програму він реалізував на тематичних форумах, а надалі його розробку використовували інші хакери для атак іноземних кампаній та подальшого скоєння кіберзлочинів. Паралельно злочинець застосовував іншу програму, яка штучно підвищувала рейтинг та пошукову видачу веб-сторінки в обхід правил використання та просування веб-ресурсів пошукових систем. За наслідками задокументованої протиправної діяльності фігуранту була оголошена підозра у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 361-1 (створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України [16].

У фокусі уваги спецслужб рф перебуває не лише Україна.

У травні 2023 року в США, за результатами проведення спецоперації під кодовою назвою “MEDUSA”, було виявилено та знищено шпигунське програмне забезпечення російського походження. Представники Міністерства юстиції США та ФБР анонсували, що вимкнули частину ШПЗ, яке російські спецслужби використовували для викрадення секретів та конфіденційних даних із США та країн НАТО протягом останніх 20 років. Встановлено, що 16-й Центр фсб рф використовув хакерське угрупування “Turla” з метою поширення програмного забезпечення “Snake”для викрадення конфіденційної інформації від урядових установ та відомств США й НАТО, оборонних компаній, міністерств закордонних справ, медіа-організацій та високотехнологічних дослідницьких установ. Загалом, “кремлівські” шпигуни використовували ретельно розроблену комп’ютерну програму для викрадення інтелектуальної власності та конфіденційної інформації у більш ніж в 50 країнах світу [17].

Виходячи із викликів та загроз у кібердомені, 16 травня 2023 року Україна нарешті офіційно приєдналася до Центру НАТО з питань співробітництва в галузі кіберзахисту (CCDCOE). Центр НАТО з питань співробітництва в галузі кіберзахисту забезпечує комплексну боротьбу з кібератаками, гарантує кіберзахист інформаційних систем, а також є профілюючою структурою щодо навчання та підготовки фахівців з кіберзахисту НАТО. Наразі Центр налічує 20 учасників – 17 членів Альянсу і три країни-партнери. Такий важливий крок дозволить посилити національні спроможності у сфері забезпечення кібербезпеки та впровадити кращі практики міжнародного досвіду у питаннях теоретичної підготовки та практичної складової посилення кіберзахисту [18].

Як переконливо засвідчує сучасний досвід, забезпечення національної безпеки неможливе без удосконалення вітчизняної системи забезпечення кібербезпеки, яка би відповідала критеріям членства України в НАТО, підтримки міжнародних ініціатив у сфері кібербезпеки, інтенсифікації співпраці України з ЄС та НАТО з метою посилення спроможностей сектору безпеки і оборони у сфері кібербезпеки, участі у відповідних міжнародно-правових заходах. Базові засади співробітництва НАТО з державами-партнерами у сфері кіберзахисту передбачають, що Альянс надаватиме країнам-партнерам свою експертну допомогу та, потенційно, свої спроможності для захисту від кібератак. При цьому, країни-партнери можуть звертатися з пропозиціями щодо отримання підтримки з боку НАТО у випадках кібератак національного значення. Конструктивна співпраця між НАТО та Україною є взаємовигідною у тому сенсі, що Альянс може надати інформацію та підтримку партнерам, але, у свою чергу, може отримати необхідну інформацію та підтримку від партнерів, зокрема, що стосується обміну досвідом у сфері забезпечення кібербезпеки; НАТО і партнери повинні уникати дублювання заходів, що вживаються в рамках інших міжнародних організацій, які залучаються до захисту інформаційних систем від кібератак; наявність Угоди про безпеку між НАТО та країною-партнером, в якій визначатимуться обсяги допомоги та інформаційного обміну тощо.

Висновки.

В умовах війни, комплексний характер кіберпростору вимагає спільних й концентрованих зусиль держави, приватного сектору, експертного середовища, технічної спільноти, зокрема кібердобровольців з протидії сучасним кіберзагрозам. Масштаби поширення ШПЗ постійно та динамічно зростають. Серед найвідоміших видів ШПЗ, які використовуються під час проведення кібератак – віруси, трояни, програми-вимагачі, хробаки тощо. У цьому контексті можна виокремити загрозливі тенденції використання державою-агресором ШПЗ.

По-перше, федеральні спецслужби рф за допомогою армії хакерів застосовують ШПЗ з метою посягання на державні інформаційні ресурси та на шкоду національній безпеці. По-друге, на системній основі, з використанням шкідливих програм, спецслужби рф прагнуть спричинити та заподіяти масштабні збитки, вразити комп'ютерні мережі органів державної влади, місцевого самоврядування, отримати несанкціонований доступ до важливих державних та комерційних інформаційних ресурсів, здійснювати крадіжки конфіденційної або службової інформації, вивести з ладу важливі об'єкти критичної інфраструктури. По-третє, у фокусі хакерських атак перебуває не тільки державний сектор, але і український бізнес, що вимагає посилення державно-приватного партнерства у цій площині. По-четверте, на російський уряд та спецслужби рф працюють чисельні групи хакерів, які виконують злочинні вказівки навколо світу, хоча у фокусі їхньої прискіпливої уваги перебуває переважно Україна, у зв'язку з чим ними, на постійній основі, розробляється та удосконалюється відповідне шкідливе програмне забезпечення, відбувається пошук нових технологічних рішень та методик, у зв'язку з чим ворога не можна недооцінювати.

Виходячи із викладеного, враховуючи той факт, що в Україні, на рівні законів, відсутні положення, які би 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, доцільним вбачається схвалення законопроекту "Про внесення змін до Закону України "Про електронні комунікації" (щодо протидії фішингу)" від 28.04.23 р. № 9250 [19]. Цей законопроект містить положення, спрямовані на системну протидію фішингу та фішинговим веб-сайтам шляхом надання повноваження центральному органу виконавчої влади у сферах електронних комунікацій та радіочастотного спектра розробити та затвердити на підставі пропозицій Національного банку України правила протидії фішингу та фішинговим веб-сайтам, встановити права та обов'язків постачальників DNS, а також визначити на законодавчому рівні такі поняття як "фішинг" та "фішинґовий веб-сайт".

Використана література

1. Антоненко Н., Дігтяр Я., Крикун Н. Сучасні методи боротьби з комп'ютерними вірусами. *Економіка та суспільство.* 2022. Вип. № 43. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1739/1674

2. Білан І.А. Особливості застосування ШПЗ спецслужбами країни-агресора. *Інформація і право.* № 2(45)/2023. С. 139-152.

3. Бойко В.Д., Василенко М.Д., Золотоверх Д.С. Безпека комп'ютерних систем в контексті законодавства та запобігання кіберзагрозам. *Юридичний вісник.* 2019. № 2. С. 70-76.

4. Василенко М.Д., Радчук В.О., Слатвінська В.М. Шкідливі програми в контексті розуміння комп'ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження. *Наукові праці Національного університету "Одеська юридична академія".* 2021. Т. 28. С. 28-36.

5. Волков 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.

6. Жульковська І., Плужник А., Жульковський О. Сучасні методи виявлення шкідливих програм. *Математичне моделювання.* 2021. № 1 (44). С. 46-54.

7. Користін О.Є., Користін О.О. Загрози у сфері кібербезпеки України. *Наука і правоохорона*. 2022. № 1(55). С. 119-126.

8. Лисенко С.М., Щука Р.В. Аналіз методів виявлення ШПЗ в комп`ютерних системах. *Вісник Хмельницького національного університету.* 2020. № 2. С. 101-107.

9. Поліщук Л.І. Дослідження засобів боротьби з комп'ютерними вірусами для захисту інформаційно-комунікаційних систем. *Інформаційні технології та комп'ютерна інженерія.* Кіровоград: КНТУ, 2014. С. 173-175.

10. Поляков О.М. Сучасні тренди виявлення та протидії застосуванню шпигунських та шкідливих програм. *Інформація і право.* № 2(45)/2023. С. 125-138.

11. Ричка Д.О. Комп'ютерні віруси – шкідливі програмні засоби, рушійна сила модифікації. *Науковий вісник Херсонського державного університету*. 2018. Вип. 1. Т. 2. С. 89-93.

12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

13. Стартував проєкт із протидії кібершахрайству у фінансовому секторі URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori

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

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

16. Кіберполіцейські викрили жителя Чернівців у розробці та збуті ШПЗ. URL: https://www.npu.gov.ua/news/kiberpolitseiski-vykryly-zhytelia-chernivtsiv-u-rozrobtsi-ta-zbuti-shkidly voho-prohramnoho-zabezpechennia

17. У США знищили шпигунське програмне забезпечення ФСБ. URL: https://www.unn. com.ua/uk/news/2026746-u-ssha-znischili-shpigunske-programne-zabezpechennya-fsb

18. Україна офіційно приєдналася до Центру кіберзахисту НАТО. URL: https://www. ukrinform.ua/rubric-technology/3710022-ukraina-ficijno-priednalasa-do-centru-kiberzahistu-nato.html

19. 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

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