УДК 342.951

ГУРЖІЙ С.В., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-3642-4975.

ОРГАНІЗАЦІЙНО-ТЕХНІЧНИЙ АСПЕКТ ПРОТИДІЇ ФІШИНГУ

DOI...

Анотація. *Визначено поняття та види фішингу, його особливості. Деталізовано зміст та специфіку проведення фішингових атак. Узагальнено процедурні питання технологічного змісту щодо скоєння фішингу. Розглянуто алгоритм виявлення шкідливих фішингових повідомлень електронної пошти. Висвітлено традиційні методи протидії фішинговим атакам. Визначено загальні рекомендації запобігання фішингу. Запропоновано шляхи удосконалення вітчизняного законодавства з метою посилення спроможностей держави у сфері протидії фішингу.*

Ключові слова: *шкідливе програмне забезпечення, фішинг, фішингова атака, аутентифікація, конфіденційна інформація, облікові дані, блокування доменів фішингових сайтів.*

Summary. *The definition and types of phishing are determined. The specifics of the phishing attacks were detailed. The procedural technological issues in relation to phishing have been clarified. The algorithm for detecting bad phishing emails has been reviewed. The traditional methods of countering phishing attacks are shown. The general recommendations were made to prevent phishing. The directions of improvement of national legislation with the aim of strengthening the powers of the state to combat phishing are proposed.*

Keywords: *malware, phishing, phishing attack, authentification, confidential information, credentials, blocking of phishing sites domains.*

Постановка проблеми. Війна – це не тільки танки, гармати, літаки. Сучасна війна вже давно перейшла у кібернетичний вимір. Більшість мереж та систем можна зламати, а більшість програмного забезпечення має свої недоліки, які можна використати зі злочинною метою. Когнітивна війна – це вже не новомодне словосполучення. Це сучасна концепція шостого поля бою, яка вже відпрацьовується на території нашої держави. У сучасному кіберсвіті, який також охоплений агресією з боку рф, важлива роль відводиться поширенню шкідливого програмного забезпечення, особливо фішингу. Саме фішинг є великою загрозою для суспільства та більшості держав світу, що провокує необхідність посиленого захисту користувачів. В умовах кібервійни, яку веде держава-агресор проти України, проблематика поширення шкідливого програмного забезпечення та, зокрема, фішингу є відкритою та своєчасною. З цією метою кремль залучає технічних експертів, хакерів, та підготовлених ІТ-спеціалістів а вітчизняний кіберпростір потерпає від ворожих загроз та хакерських атак.

Саме тому, майбутні війни ще більше будуть переходити у домен кіберпростору. Під час воєнного стану шахраї та хакери під триколором дедалі частіше використовують фішингові сайти, які маскують під ресурси для оформлення соціальних виплат від держави, фондів, міжнародних організацій. За таких умов актуальним залишається висвітлення проблемних питань удосконалення вітчизняної моделі організаційно-технічного забезпечення протидії фішингу.

Результати аналізу наукових публікацій. Методологічне забезпечення процесів виявлення фішингу досліджували А. Жилін [1], Д. Мехед, Ю. Ткач, В. Базилевич [4].

Фішинг з позиції шахрайства був предметом поглибленого наукового пошуку І. Доміонової [2], О. Косаревської, К. Фаркаш [3], П. Поповської та О. Карачевцева [5]. Правові проблеми протидії фішингу розглядали у своїх працях І. Яковюк, А. Волошин, А. Шовкун [7], О. Самойленко [6] та ін. Проте детальний огляд організаційно-технічних засад протидії фішингу в умовах правового режиму воєнного стану не був предметом окремого дослідження. Це свідчить про актуальність тематики цієї статті.

Метою статті є уточнення організаційно-технічної моделі протидії фішингу в умовах кібервійни, висвітлення особливостей запобігання використанню фішингу хакерами та кіберзлочинцями в контексті визначення шляхів законодавчого удосконалення протидії фішингу.

Виклад основного матеріалу. Фішинг (від англ. *phishing* – "риболовля", "видобування") – це вид Інтернет-шахрайства, який полягає в крадіжці конфіденційних даних користувачів. Простіше кажучи, зловмисники "розводять" користувачів на те, щоб вони самі розкрили свої персональні дані щодо номерів телефонів, номерів та кодів банківських карт, логінів, паролів 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. Загалом фішинг – це тип кібератаки, під час якої зловмисник видає себе за авторитетну організацію або компанію для того, щоб ошукати людей та зібрати їхню конфіденційну інформацію, зокрема, таку як, дані кредитних карток, імена користувачів, паролі.

Оскільки фішинг використовує психологічні маніпуляції та базується на людських помилках (а не на апаратному або програмному забезпеченні), він вважається типом атаки соціальної інженерії. Він заснований на незнанні користувачами елементарних законів мережевої безпеки. 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 їх грошей. 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.

Спецслужби РФ та їх сателіти цілеспрямовано використовують 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 антивірусні програми. Фсб за допомогою армії хакерів систематично з використанням шкідливих програм має за мету спричинити масштабні збитки, вразити та заблокувати комп'ютерні мережі органів державної влади, місцевого самоврядування та максимально вивести з ладу об'єкти критичної інфраструктури. Хакери використовують нові розробки шкідливого програмного забезпечення для потужних кібератак не лише на державний сектор, але і на український бізнес. Тому актуальним та найбільш простим методом поширення шкідливого програмного забезпечення залишається саме 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 її 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 ІТ-інфраструктури державного органу або певної компанії та заволодіти конфіденційними даними реальні. Майже неможливо гарантувати повноцінний захист від усіх типів нападів. Більшість кібератак здійснюється зловмисниками продумано та планується заздалегідь. Вони готуються і використовують для цього спеціальне програмне забезпечення. Щоб попередити та знизити можливі ризики бажано посилювати кібербезпеку на усіх рівнях. Зазвичай, фішингові атаки використовують шахрайські електронні листи, які переконують користувача ввести конфіденційну інформацію на шахрайському веб-сайті. Ці електронні листи вимагають або просять користувача надати свій пароль або підтвердити інформацію про свою кредитну картку. Така інформація надходить до підробленого веб-сайту, який дуже схожий на оригінальний.

Досить часто фішинг поширюється через листи електронною поштою, в яких вказується який-небудь важливий або вкрай привабливий контент. Для виманювання даних користувачів зловмисники використовують спеціальні методи, завдяки чому фальшиві сторінки дуже схожі на свої легітимні аналоги. Тому громадяни можуть і не помітити різницю [8].

Основними видами фішингу є клон-фішинг, цільовий фішинг, фармінг. Також активно використовується таргетований фішинг, який залишається одним із домінантних і ефективних методів отримання доступу до інформаційних ресурсів 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 та кіберзлочинці 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 перебувати у повній безпеці. Передусім, у зоні ризику – компанії, які надають послуги та сервіси операторам критичної інформаційної інфраструктури: розробники, Інтернет-провайдери тощо.

Проблема фішингу залишається актуальною, коли йдеться про корпоративну інформаційну безпеку. Саме фішинг використовується у 75 % хакерських атак. Це свідчить про те, що саме фішинг залишається основним способом проникнення в ІТ середовище організацій та державних структур. Кінцевою метою фішингу є отримання доступу до конфіденційних даних користувачів (логіну та паролю) або шахрайським способом створення передумов для того, щоб примусити завантажити користувача шкідливий файл на свій мобільний телефон, ПК або інший пристрій. Посилання на підробний сайт або на інфікований шкідливою програмою об’єкт можуть міститися у листі або у приватному повідомлені у месенджерах або соціальних мережах. Отримавши доступ до облікових даних корпоративного користувача або завантажуючи шкідливу программу на його ПК, зловмисник у підсумку може отримати доступ до інфраструктури організації. Так, за статистикою майже 80 % успішних атак у державних організаціях починалися саме з фішингу. Низький рівень обізнаності про сучасні кіберзагрози призводить до того, що співробітники дедалі частіше попадаються на хитрощі хакерів. Саме фішинг є одним із способів розсилки так званих шифрувальників. Це програми, які шифрують файли на ПК або сервері та блокують його. За отримання ключів розшифрування файлів зловмисники вимагають викуп. Навіть якщо викуп сплачено, то

дані швидше за все будуть втрачені, що може ймовірно призвести до великих збитків, удару по репутації або інших проблем. А якщо заплатити викуп, то немає жодної гарантії, що ключі шифрування взагалі надішлють зловмисники. Фішингові розсилки можуть загрожувати будь-якій організації, державному органу, великим підприємствам. Різниця лише полягає у тому, хто проводить атаку: високопрофесійне хакерське угрупування або менш кваліфіковані зловмисники. Особливо ризикують ті організації, які не можуть собі дозволити утримувати штат ІТ-спеціалістів, які мають навички обслуговування засобів захисту інформації, швидко реагувати у випадку кібератаки та мінімізувати катастрофічні наслідки інциденту. У зв'язку з цим державні структури дедалі активніше переходять на елекронний документообіг. Цим можуть скористатися зловмисники, здійснюючи розсилку під виглядом електронних звернень до державних органів. Стати жертвою фішингу можуть також компанії, які займаються Інтернет- торгівлею та приймають заявки на поставку товарів за допомогою електронної пошти.

Фішингові атаки – найпоширена проблема мережевої безпеки, з якими стикаються як окремі особи, так і компанії. Будь то отримання доступу до паролів, кредитних карт або іншої конфіденційної інформації, хакери використовують електронну пошту, соціальні мережі, телефонні дзвінки та будь-які доступні засоби зв'язку для крадіжки цінних даних. Бізнес, звичайно ж, є особливо ласою метою. Фішингові атаки також активно використовуються навіть в криптовалютній екосистемі, де зловмисники намагаються вкрасти "Bitcoin" або інші цифрові валюти у користувачів. Наприклад, це може бути зроблено зловмисником, який підміняє реальний веб-сайт і змінює адресу гаманця на власний, створюючи в користувачів враження, що вони платять за офіційну послугу, коли насправді вони віддають свої гроші злочинцям. Фішинг – один з найпоширеніших способів кібератак, які використовує держава-агресор. Не дивлячись на те, що фільтри електронної пошти основних 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 підтвердження за допомогою інших засобів зв'язку з метою з'ясування факту того, що відправник та запит є офіційними. За правилами кібергігієни забороняється відкривати посилання в електронних листах про порушення безпеки та переходити на веб-сторінку на своїх умовах, а також доцільно слідкувати за HTTPS на початку URL-адреси. На цьому фоні кількість фішингових атак постійно зростає через повномасштабне вторгнення рф в Україну, що потребує вжиття ефективних контрзаходів.

Слушно вказує С. Ратушняк, що специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, e-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама. Користувач отримує пропозицію зареєструватися для отримання будь-якої вигоди або підтвердити свої персональні дані нібито для банківських або комерційних установ, клієнтом яких він є. Як правило, шахраї маскуються під відомі компанії, додатки соціальних мереж, сервіси електронної пошти. Електронна адреса відправника дійсно схожа на адресу знайомої користувачеві компанії [9, с. 183].

Здатність виявляти та ізолювати шкідливі фішингові повідомлення електронної пошти є великою проблемою як з технічного, так і з управлінського боку. З метою захисту від фішингових листів загалом буде корисною система обслуговування електронної пошти з вбудованими розширеними функціями безпеки. Як правило, в систему включені функції безпечних вкладень та безпечного посилання. Така система

електронної пошти просканує посилання та визначить, безпечна вона чи ні, перш ніж перенаправити користувача на веб-сайт, а потім 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. Коли справа доходить до ІТ-безпеки та протидії фішингу, одна з найсерйозніших проблем – це здатність виявляти проблеми в мережі, а потім визначати ці проблеми, блокувати їх та вирішувати.

Традиційні методи протидії фішинговим атакам передбачають: 1) розробку унікального дизайну сайту, що передбачає вибір клієнтом під час укладання договору з банком індивідуального дизайну зображення. У випадку, якщо під час входу на сайт банку клієнт не бачить це зображення, то він має негайно покинути сайт та попередити про це службу безпеки банку; 2) використання одноразових паролів, тобто на відміну від класичого паролю, одноразовий використовується виключно тільки один раз, а потім користувач вводить новий пароль; 3) одностороння аутентифікація передбачає використання протоколу безпечних з'єднань SSL (Secure Sockets Layer), що, у свою чергу, забезпечує захищений обмін даними між певним веб-сервером та користувачами. Навіть попри той факт, що протокол дозволяє аутентифікувати не тільки сервер, але й користувача, на практиці все ще застосовується тільки одностороння аутентифікація. Для встановлення SSL-з'єднання необхідно, щоб сервер мав цифровий сертифікат, який використовується для аутентифікації. Сертифікат зазвичай видається та завіряється третьою стороною, в ролі якої виступають відповідні центри сертифікації. Їхня роль полягає у тому, щоб підтвердити дійсність веб-сайтів різних компаній, формувати довіру до них, сприяти можливості перевіряти дійсність сайтів, власники яких зареєстровані у цьому центрі сертифікації. Узагальнюючи викладене, основним пріоритетом під час побудови захисту від фішингу є мінімізація залежності від людського фактору. Співробітники, які є кінцевими користувачами листів фішингу, є останньою ланкою захисту компанії від атак на систему безпеки. У цьому контексті життєво важливо, щоб працівники пройшли належне навчання та мали розуміння як розпізнавати такі електронні листи та реагувати на них. Добра поінформованість та знайомство з шаблонами фішингових листів дозволить їм захиститися. Тим часом, організації та державні структури також повинні мати можливість виявляти найбільш уразливих співробітників та проводити відповідне навчання на кшалт загальної програми навчання на рівні організації.

Рішення захисту від фішингу та шифрувальників також передбачають три варіанти – базовий, покращений та максимальний. Базовий передбачає захист електронної пошти за допомогою відповідного шлюзу. Вважається, що найбільш перспективною є реалізація шлюзових рішень, які спрощують процедури адміністрування та надають змогу надійно закрити усю комп'ютерну мережу тієї чи іншої організації. Тобто, перш за все, доцільно встановити фільтруючий шлюз для того, щоб листи електронної пошти проходили ретельну перевірку перед тим, як потрапити до поштових скриньок співробітників. Сучасні рішення надають змогу надати відсіч масовим фішинговим розсилкам. Також на рівні шлюзу можлива фільтрація контенту та уникнення уразливостей "MailSploit", які потенційно можуть відкривати доступ до комп'ютерів жертв шляхом відкриття спеціально підготовлених повідомлень. Єдине ефективне рішення – автоматизація процесу тестування інфраструктури на предмет уразливості фішинговим атакам.

Сучасні ефективні шлюзові рішення надають змогу боротися з атаками на чотирьох рівнях: 1) рівень доступу, тобто основа антифішингової безпеки, який передбачає запровадження URL-фільтрації (заборона доступу до вебсайтів з категорії фішингових), що дозволяє відрізнити посилання на фішинговий сайт від легітимного, здатна протидіяти фішингу. Фільтрація сайтів застосовується з метою обмеження нецільового використання мережі Інтернет співробітниками для захисту від фішингових атак; 2) рівень активного контенту, що передбачає реалізацію фільтрації HTML-коду та інших об'єктів щодо наявності шкідливого коду, закритих каскадних переадресацій, на випадок коли тіло трояна збирається із невеликих нешкідливих та таких, що важко виявляються, фрагментів на декількох сайтах, по яких користувача обдурюють; 3) рівень комунікацій, який використовується коли метою залучення користувача на підроблений сайт є інфікування його комп'ютера будь-яким шкідливим кодом. Ще одним рівнем блокування захисту може бути недопущення передачі приватних даних, які зібрали боти. Навіть попри велку кількість видів троянів та ботів, існує лише декілька десятків комунікаційних протоколів, за якими вони здійснюють взаємодію із своїм центром керування. Блокування таких комунікацій найбільш ефективно здійснюється по сигнатурах протоколів, а не самого шкідливого коду; 4) рівень передачі даних отримав широке поширення завдяки DLP-рішенням (Data Leak Prevention), що надає змогу у рамках певної організації побудувати ще один рубіж оборони у вигляді контролю потенційних каналів витоку даних. Такі рішення можуть допомогти у виявленні та недопущенні відправки шкідливого коду, наприклад, номеру кредитної карти або іншої конфіденційної інформації.

Узагальнюючи викладене, доцільно вказати, що на базовому рівні захист здійснюється тільки щодо можливостей електронної пошти. Покращений рівень передбачає додатковий захист від мережевих загроз. На цьому рівні забезпечується додаткова протидія фішингу та шифрувальникам. Наприклад, коли шахрайське посилання приходить в особистому повідомленні у месенджері, а не у листі. Користувач відкриває таке посилання у браузері. Максимальна безпека – спеціальна платформа для навчання та перевірки навичок кіберграмотності співробітників. Тобто користувач може відкрити фішингове посилання на особистому пристрої, що залишиться непоміченим для корпоративної мережі захисту. Якщо ж співробітники навчаться самостійно виявляти фішинг, у зловмисників не буде шансів досягти своїх цілей. У всіх трьох варіантах кінцевою метою є удосконалення захисту від загроз. тобто створення віртуального та ізольованого середовища для перевірки потенційно шкідливих файлів. Це дозволяє забезпечити ешелоновану безпеку: навіть якщо файл пройде фільтр електронної пошти або систему боротьби з мережевими загрозами, то він буде виявлений у ізольованому середовищі, а при необхідності – заблокований.

Єдиним слабким місцем для вказаних систем може бути неможливість захисту мобільних співробітників, які працюють віддалено за відкритими каналами зв'язку. Для вирішення цієї проблеми у якості можливого варіанту є проксирування, тобто вихід до мережі Інтернет з ноутбуків компанії тільки через головний офіс. Таке рішення з метою спрощення адміністрування та зниження фінансових витрат також э актуальним для філій та відділень організацій. Також важливим рішенням є відмова від паролів під час доступу користувачів до рахунків та використання цифрових сертифікатів, що робить прослуховування та перехоплення трафіку неможливим.

Основою безпеки під час використання цифрових сертифікатів є збереження закритого ключа. Тобто необхідно мати фінансові та технічні можливості щодо надійного захисту закритого ключа, який використовується для аутентифікації. Зберігання свого закритого ключа у реєстрі операційної системи на жорсткому диску не є надійним та

безпечним. У випадку інфікування комп'ютера користувача ці дані можуть бути викрадені шкідливим програмним забезпеченням, а захист закритого ключа паролем не буде надійною гарантією збереження грошових коштів та даних користувача. Надійним засобом зберігання закритих ключей користувача є використання криптографічних токенів. На відміну від інших зовнішніх носіїв (наприклад, USB-флеш), під час користування токенами відсутня необхідність у копіюванні конфіденційної інформації до оперативної памяті комп'ютера під час проведення операції з аутентифікації, оскільки такі пристрої не тільки надійно зберігають закриті ключі, але й апаратно виконують необхідні криптографічні обчислення. При цьому важливо, що використати токен може тільки його власник, який знає його пароль (PIN-код). В сучасних умовах чимало банків пропонують своїм клієнтам можливість аутентифікації не тільки за разовими паролями, але й з використанням цифрових сертифікатів, оскільки використання апаратних криптографічних токенів з метою підвищення безпеки зберігання закритих ключів не отримало поки широкого поширення.

Виявлення фішингових сайтів та внесення їх до чорних списків займаються чимало компаній – від виробників антивірусних програм до банківських установ, платіжних систем та правоохоронних органів. Також утворюються спеціальні організації для боротьби з фішерами, наприклад Anti Phishing Work Group (APWG - http://www.apwg.org). Спільні заходи зацікавлених сторін у тісній співпраці з реєстраторами та хостинговими компаніями надають змогу оперативно закривати підробні сайти. Реальні зусилля спрямовані на максимально швидке оновлення чорних списків та блокування роботи сайтів зловмисників. Середня тривалість життя фішингового сайту складає орієнтовно 49 годин. Проте не усі виробники антивірусного захисту можуть мати технічні можливості оперативного оновлення баз та швидко блокувати фішингові сайти. На жаль, чимало користувачів нехтують елементарними засобами кібергігієни та не мають взагалі антивірусного захисту на своїх комп'ютерах, вводять номери кредитних карт та іншу конфіденційну інформацію з випадкових робочих місць. Реальні атаки можуть спричинити суттєві збитки тому чи іншому користувачу, організації або компанії (навіть довести до банкрутства).

Також існують загальні рекомендації щодо запобігання фішингу. По-перше, доцільно завжди перевіряти адресний рядок у своєму браузері, ніколи не переходити за посиланнями у сумнівному листі. У разі сумнівів треба перейти на сторінку, вказану в тексті електронного листа, через стартову сторінку відповідної організації, тобто не вводячи посилання, вказане в адресному рядку браузера. По-друге, забороняється повідомляти особисті дані, такі як паролі, номери кредитних карток або транзакцій, електронною поштою – незалежно від того, наскільки достовірним є цей електронний лист. По-третє, категорично не можна запускати посилання для завантаження прямо з електронного листа, на справжність якого не можливо повністю покластися. Зокрема, ніколи не можна відкривати файли, прикріплені до підозрілого листа. По-четверте, під час завершення кожної онлайн-сесії необхідно виходити із системи, а не просто закривати вікно браузера. Ніколи не вводити особисті дані на веб-сайтах із незашифрованим з'єднанням та завжди перевіряти актуальність антивірусного програмного забезпечення та працездатність міжмережевого екрану. Так, важливо, що на фішинговий сайт може вказувати будь-яка відмінність у URL-адресі (зайві символи, невірне написання). Користувачам варто завжди звертати увагу на адресу необхідного сайту, а також не переходити за підозрілими гіперпосиланнями і не вводити конфіденційні дані. Наприклад, для онлайн-шопінгу рекомендується використовувати перевірені сайти, а інформацію щодо соціальних виплат отримувати лише з офіційних сторінок державних органів.

Схеми з використанням фішингу зловмисники можуть використовувати і на платформах оголошень. Тому при купівлі-продажу товарів, треба уважно обговорювати деталі угоди лише у чаті цієї платформи і не переходити у сторонні месенджери.

Протягом 2022 року Національний банк України виявив понад 4500 фішингових сайтів, які збирали інформацію про громадян. Після початку повномасштабного вторгнення різко зросла кількість ошуканих у мережі громадян. Це спонукало Національний банк України запровадити захід протидії шкідливим сайтам, а його практичне впровадження сприятиме посиленню кіберзахисту фінансової системи, що надасть змогу убезпечити українців від аферистів, а в майбутньому – зменшити кількість фішингових атак та загалом обсяги фінансового шахрайства в Україні. Відповідальною державною структурою у сфері боротьби з фішингом визначено Національний координаційний центр кібербезпеки при РНБО України. На початку 2023 року РНБО України спільно з Національним банком України запустили відповдний проект із протидії кібершахрайству у фінансовому секторі. Тільки за перший місяць роботи проекту було зафіксовано понад 120 тисяч унікальних переходів на сторінку, що попереджає про загрозу крадіжки даних. Саме 15 лютого 2023 року Національний координаційний центр кібербезпеки (НКЦК) при РНБО України спільно з Національним банком України 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 – зменшення переходу користувачів на шахрайські сайти шляхом перенаправлення їх на сторінку із попередженням, що сайт створений або контролюється зловмисниками. Національною комісією, що 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) “Про впровадження системи фільтрації фішингових доменів” від 30.01.23 р. № 67/850 [10], яке було опубліковане на веб-сайті НКЕК до відома та виконання постачальниками електронних комунікаційних мереж та послуг-провайдерами DNS.

Цим розпорядженням також було схвалено Регламент роботи системи фільтрації фішингових доменів. Саме на підставі цього розпорядження була створена централізована система автоматичного блокування Інтернет-ресурсів, що, за задумом, 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. У рамках нормативних вимог з 2 березня 2023 року в Україні усі без виключення 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". 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.

Інтернет-асоціація України закликає терміново скасувати розпорядження НЦУ від 30.01.23 р. № 67/850 [10] з метою опрацювання альтернативних шляхів протидії фішингу з прийнятим рівнем ризику, виходячи із кращих практик зарубіжного досвіду. Викликав обурення та піддався жорсткій критиці з боку Інтернет- асоціації України й проект закону "Про внесення змін до Закону України "Про електронні комунікації" (щодо протидії фішингу)" від 28.04.23 р. № 9250 [11], оскільки встановлення національного "firewall" може призвести до довільного блокування будь-яких Інтернет-ресурсів. Законопроєкт № 9250 спрямований на протидію фішингу та фішинговим веб-сайтам шляхом надання відповідних повноважень центральному органу виконавчої влади у сферах електронних комунікацій та радіочастотного спектру. За законопроектом цей орган зобов'яжуть розробити та затвердити правила протидії фішингу, встановити права та обов'язки постачальників DNS. У свою чергу, в організації стверджують, що законопроєктом буде встановлено не передбачений Конституцією вид неправомірного діяння, який не є ані злочином, ані адміністративним чи дисциплінарним правопорушенням. На переконання представників Інтернет-асоціації України, цей законопроект має на меті легалізувати вже побудовану, незаконно функціонуючу під управлінням НКЦК РНБОУ систему блокування доменів. Така система має ризики для кібербезпеки держави, оскільки держава-агресор, отримавши незаконний доступ, може заблокувати в Україні доступ до веб-ресурсів. Крім того, організація нагадує про корупційні ризики під час прийняття рішень щодо включення сайтів до переліку заблокованих доменів та про ризики для свободи слова, оскільки цей механізм може бути використаний для блокування будь-яких онлайн-медіа. За таких умов, актуальною є боротьба з фішинговими сайтами у форматі налагодження роботи та легалізації системи методичного блокування доменів фішингових сайтів на рівні DNS-серверів.

За попередніми оцінками, ця система дозволила попередити збитки для громадян України на суму понад 5 млн. гривень тільки за 3 місяці 2023 року, тобто починаючи з 2 березня 2023 року в Україні розпочала працювати система фільтрації фішингових доменів, яку запровадив Національний центр оперативно-технічного управління телеком-мережами (НЦУ), орган, відповідальний за телекомунікації в країні під час війни. Тобто держава активно опікується проблематикою протидії фішингу, особливо в умовах правового режиму воєнного стану.

Висновки.

З кожним днем наше середовище стає більш цифровим та одночасно небезпечним. В умовах цифровізації та швидкого доступу до інформації формується чимало схем

шахраїв, які намагаються викрасти або отримати доступ до банківських карток, персональних даних та до соціальних мереж. Фішинг є найбільш простим та у той самий час найбільш небезпечним способом кібератаки в мережі Інтернет. На жаль, жодна операційна система не може протидіяти таким атакам. Саме фішинг залишається найпоширенішим методом шахрайства та засобом привласнення коштів і персональних даних. Фішинг – один з найпоширеніших методів шахрайства в мережі Інтернет, який використовують кіберзлочинці для привласнення коштів та збору персональних даних.

Після російського широкомасштабного воєнного вторгнення на територію України 24 лютого 2022 року проблема фішингових атак та розроблення механізмів їх протидії є особливо актуальною. Серед тем, які використовують зловмисники, активно використовується тематика фінансової допомоги громадянам України від державних органів та міжнародних організацій. За результатами аналізу, діяльність більшості шахрайських груп, які працюють в Україні, координується злочинцями з рф, які надають типові шаблони фішингу, способи виведення коштів тощо. У рамках гібридної війни спецслужби рф створюють різноманітні фішингові сайти з метою збору персональних даних громадян України, волонтерів, військовослужбовців та членів їх сімей під виглядом заявок на допомогу. Отже, фішинг становить значну загрозу для національної безпеки України. Адже десятки зловмисних груп, які проводять фішингові кампанії проти українських громадян, координуються російськими злочинцями, а фсб сприяє їх діям. Внаслідок цього кошти, які втрачають українці, використовуються для підтримки держави-агресора та фінансування тероризму.

У зв’язку з цим наша держава має постійно удосконалювати організаційно-технічну модель протидії фішингу. Проте, в Україні на рівні законів, відсутні положення, які б містили, в першу чергу, превентивні заходи для користувачів мережі Інтернет. Потребують визначення й додаткові обов’язки для постачальників електронних комунікаційних послуг, а також основоположні правила протидії фішингу та фішинговим веб-сайтам. Таким чином, доцільним вбачається прискорити схвалення законопроекту “Про внесення змін до Закону України “Про електронні комунікації” (щодо протидії фішингу)” [11], що надасть змогу ввести в законодавче поле такі поняття, як “фішинг” та “фішинґовий веб-сайт”, посилити на державному рівні системну боротьбу з фішингом, запровадити відповідні правила протидії фішингу та фішинговим веб-сайтам, а також встановити права та обов’язки постачальників DNS.

Прийняття цього законопроекту необхідне для вирішення питань протидії фішингу, в першу чергу, протидії кіберзлочинцям, які отримають інформацію у користувачів в мережі Інтернет про їх дані у банківських та фінансових установах, створюють в мережі Інтернет фальшиві веб-сайти, які, зазвичай, можуть повністю копіювати дизайн банків, фінансових установ, сервісів обміну валют, служб доставки тощо. У разі набуття чинності цього закону слід встановити кримінальну відповідальність за фішинг, а саме за незаконне заволодіння конфіденційними даними Інтернет-користувачів, що передбачає внесення відповідних змін до Кримінального кодексу України.

Використана література

1. Жилін А., Шевчук О. Метод аналізу фішингових повідомлень. *Information Technology and Security.* January-June 2022. Vol. 10. Iss. 1 (18). P. 72-82.

2. Доміонова І.В. Ризик шахрайства в умовах функціонування електронного банкінгу. *Бізнес навігатор.* – (Науково виробничий журнал). 2017. Вип. 4-2. С. 92-98. URL: http://nbuv.gov.ua/UJRN/bnav_2017_4-2_21

3. Косаревська О.В., Фаркаш К.В. Кіберзлочини у сфері Інтернет шахрайства: фішинг та способи його уникнення: зб. матеріалів Всеукраїнської науково-практичної конференції *Кібербезпека в Україні: правові та організаційні питання,* м. Одеса, 17 лист. 2017 р. Одеса: Одеський державний університет внутрішніх справ, 2017. С. 144-145.

4. Мехед Д., Ткач Ю., Базилевич В. Дослідження технологій впливу та методів протидії фішингу. *Захист інформації.* 2019. Т. № 21. С. 246-251.

5. Поповська П.І., Карачевцев О.В. Фішинг як одна із форм шахрайства в Інтернеті: зб. матеріалів всеукраїнської науково-практичної конференції *Актуальні питання протидії кіберзлочинності та торгівлі людьми*, м. Харків, 23 лист. 2018 р. Харківський державний університет внутрішніх справ, 2018. С. 82-84.

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

7. Яковюк І.В., Волошин А.П., Шовкун А.О. Правові аспекти протидії фішингу: досвід Європейського Союзу. *Проблеми законності.* 2020. Вип. 149. С. 9-23.

8. Ратушняк С.С. Методи захисту Інтернет від фішингу: зб. матеріалів ІІ Всеукраїнської науково-практичної конференції *Кібербезпека в сучасному світі,* м. Одеса, 20 лист. 2020 р. Одеса: Видавничий дім "Гельветика", 2020. С. 183-186.

9. Як вберегтися від фішингових атак. *Голос України.* – (29.05.22 р.). URL: http://www.golos.com.ua/article/360653

10. 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&lang uage=uk

11. 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

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