image encoding. An encryption method that used the Hadamard matrix to encrypt color raster images was identified. In the process, it was determined that it was sufficient to use non-orthogonal Hadamard base matrices, but in the future, 16 Hadamard 4x4 support matrices could be used to improve the crypto-stability of the application. An algorithm for encrypting image pixel combinations using the Hadamard matrices was developed. First, for each pixel of the image, this method randomly determines three Hadamard matrices R, G and B. Then, for each matrix of the encoded image, a matrix key is selected. The key matrix is generated in such a way that when you overlay one matrix on another, they form a combination of four pixels that are as close as possible to the pixel of the input / secret image. The R, G, and B matrices of one pixel of the encoded image and key overlap. The matrix data is then added to the encoded image and key image respectively according to the pixel position. As a result, the web application user receives two images (encoded image and key). Only one of them cannot play a secret image. A web application was developed that uses this encryption method to encode and decode color images.
Keywords: Hadamard matrix, information security, encryption, color images, web application.

Фролов Артем Олександрович, аспірант кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: artem.frolov@uzhnu.edu.ua.
Orcid ID: 0000-0003-4967-0067.
Фролов Артем Александрович, аспирант кафедры твердотельной электроники и информационной безопасности физического факультета УжНУ.
Frolov Artem, PhD student, Department of Solid State Electronics and Information Security of the Physics Faculty, UzhNU.

Чобаль Олександр Ілліч, кандидат фізико-математичних наук, доцент кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: oleksandr.chobal@uzhnu.edu.ua.
Orcid ID: 0000-0002-8042-8052.
Чобаль Александр Ильич, кандидат физико-математических наук, доцент кафедры твердотельной электроники и информационной безопасности физического факультета УжНУ.
Chobal Oleksandr, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.

Різак Василь Михайлович, доктор фізико-математичних наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
E-mail: vrizak@uzhnu.edu.ua.
Orcid ID: 0000-0002-9177-0662.
Ризак Василий Михайлович, доктор физико-математических наук, профессор, заведующий кафедрой твердотельной электроники и информационной безопасности физического факультета УжНУ.
Rizak Vasyl, Doctor of Physical and Mathematical Sciences, Professor, Head of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.

DOI: 10.18372/2410-7840.21.14338
УДК 004.056.53

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ВПЛИВУ ТА МЕТОДІВ ПРОТИДІЇ ФІШИНГУ

Дмитро Мехед, Юлія Ткач, Володимир Базилевич

У статті проаналізовано актуальні загрози інформаційній безпеці та зроблено прогноз основних напрямків проведення кібератак в майбутньому. З'ясовано, що серед існуючих загроз інформаційній безпеці вже котрий рік поспіль перші позиції займають методи соціальної інженерії. Виділено найбільш поширені інструменти і методи однієї зі складових соціальної інженерії - фішингу, зокрема вспливаючі вікна, міжсайтовий скриптинг, помилки URL-адреси тощо. Дослідниками сформульовано низку рекомендацій щодо захисту організацій та підприємств у контексті використання ефективних технічних засобів захисту (наприклад, SIEM-рішення - для своєчасного виявлення атаки, якщо інфраструктура виявилась зараженою, автоматизовані засоби аналізу захищеності і виявлення вразливостей в ПЗ, мережевий екран рівня додатків (web application firewall) як превентивний захід захисту веб-ресурсів), безпосереднього захисту даних (зокрема, збереження конфіденційної інформації у закритому вигляді з обмеженим доступом, регулярне створення резервних копії систем і збереження їх на виділених серверах окремо від мережевих сегментів робочих систем), а також безпеки персоналу (а саме, підвищення обізнаності працівників в питаннях ІБ, регулярне навчання персоналу правилам безпечної роботи в Інтернеті, пояснення методів атак і способів захисту тощо).
Ключові слова: *інформаційна безпека, соціальна інженерія, фішинг, засоби захисту інформації.*

Вступ. Фахівці в усьому світі ведуть безперервну боротьбу з кіберзлочинністю, і це, як і раніше, змушує зловмисників вдосконалювати свої інструменти. На початку минулого року кібератаки стали випробуванням для багатьох організацій різних сфер життєдіяльності. Серед існуючих загроз інформаційної безпеки вже котрий рік поспіль лідуючі позиції займають методи соціальної інженерії. Кіберзлочинці продовжують віднаходити все нові методи впливу на користувачів, які дозволили б їм заразити цільову систему шкідливим ПЗ, вкрасти гроші або отримати доступ до конфіденційної інформації тощо. Фішинг, як один з найпопулярніших серед численних інструментів соціальної інженерії, може приймати різні форми і може бути реалізований за допомогою безлічі засобів та методів.

Аналіз останніх досліджень і публікацій. Дослідженню інформаційної безпеки присвячені роботи В.В. Баранника, В.М. Богуна, С.В. Віхорева, І.Д. Горбенко, Ю.І. Грицюк, С.В. Казмирчук, Г.Ф. Конаховича, О.Г. Корченка, М.Г. Луцького, А.І. Марущака, В.П. Мельнікова, В.В. Мохора, О.М. Новікова, О.В. Олійника, О.В. Сосніна, С.В. Толюпи, В.О. Хорошко, О.К. Юдіна та ін. Публікації [2]-[5] підтверджують актуальність загроз інформаційної безпеки. Серед яких вже котрий рік поспіль перші позиції займають методи соціальної інженерії [8, 9].

Дослідження різноманітних аспектів інформаційно-аналітичної діяльності здійснювали Т.В. Абрамова, С.С. Алдишев, В.П. Александрова, А.А. Атаян, С.Ф. Багаундінова, Т.В. Вдовіна, А.В. Горячов, Р.О. Гуревич, М.І. Жалдак, О.П. Значенко, В.Г. Кальченко, Н.В. Кисіль, В.І. Клочко, Н.В. Морзе, С.Ю. Нікіфорова, О.В. Пархоменко, С.А. Раков, М.В. Селіна, Ю.М. Ткач, В.А. Сластьонін та ін.

Виклад основного матеріалу. Аналіз актуальних загроз інформаційної безпеки на основі звітів провідних компаній з кібербезпеки [7] дає можливість визначити наступні тенденції:

– Кількість унікальних кіберінцидентів продовжує рости і на 47% перевищило показники аналогічного періоду в минулого року.

– Переважали цілеспрямовані атаки - на конкретні організації та їх клієнтів, на криптовалютні біржі. В ході цих атак зловмисники були досить винахідливі. Вони не тільки використовували шкідливе ПЗ, а й шукали уразливості нульового рівня, дізнавалися паролі адміністраторів за допомогою соціальної інженерії, отримували доступ до ресурсів контрагентів.

– Продовжила рости частка кібератак, виконаних з метою отримання інформації. Причому зловмисники найбільше були зацікавлені в персональних та облікових даних, а також в даних банківських карт. Їх викрадали в основному за допомогою компрометації різних онлайн-майданчиків - інтернет-магазинів, сервісів для продажу квитків, бронювання готелів і т. п.

– Приватні особи страждали від різного шкідливого ПЗ: велику його частину вони встановлювали самі по неуважності або в результаті незнання, проте зустрічалися і такі методи атак, коли, наприклад, нові смартфони продавалися в магазині з уже встановленим в прошивку шкідливим програмним забезпеченням.

Якщо говорити про прогнози, то, ймовірно, збережеться тенденція до збільшення частки атак, спрямованих на викрадення даних. Багато компаній приділяють недостатньо уваги захисту оброблюваної інформації (особливо персональних і медичних даних), що робить її легкою здобиччю навіть для низькокваліфікованих хакерів (яких з кожним днем стає все більше). Отримана інформація потім продається на тіньовому ринку і використовується для інших кібератак.

На рис. 1 представлено результати аналізу кіберзагроз за 2019 рік. Згідно з опрацьованими нами даними найбільша частка загроз, що виникають і у сфері інформаційного безпеки, спричинені використанням шкідливого програмного забезпечення (35%), друге місце посідає соціальна інженерія, а саме 18% від загальної кількості реалізованих загроз, третє – 15%, 14% та 13% відповідно припадає на хакінг, підбір облікових записів, експлуатацію Веб-вразливостей; DDoS атаки та інші загрози становлять лише 5%.

Таким чином, вже котрий рік поспіль займають методи соціальної інженерії є одним із потужних засобів здійснення кібератак. Наприклад, у травні дослідники з Lookout розповіли про атаки на чиновників, дипломатів, військових і інших високопоставлених осіб з Пакистану, Афганістану, Індії, ОАЕ, в ході яких була викрадена важлива інформація з їх смартфонів, включаючи зображення, звукові записи і текстові повідомлення. Для того щоб заразити мобільні телефони шпигунським ПЗ, зловмисники заводили з жертвами бесіду в соціальній мережі Facebook, в ході якої ділилися фішинговою посиланням, наприклад на відеозапис, при переході через яку на смартфон встановлювалося шкідливе ПЗ з стороннього магазину додатків.

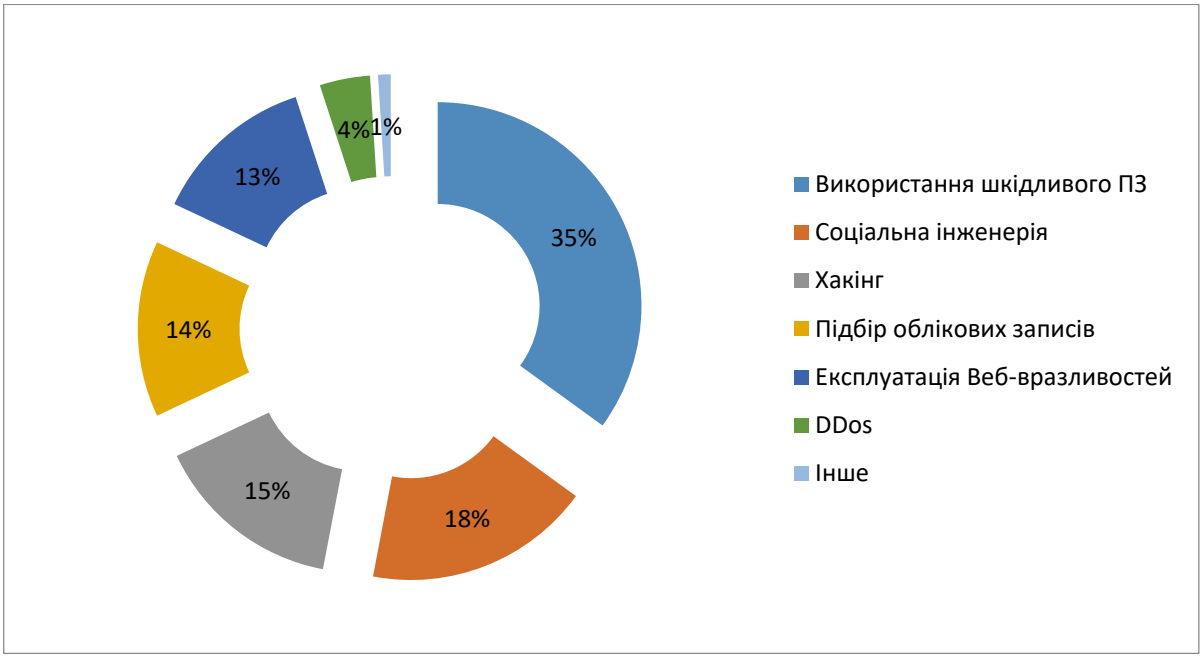

Рис. 1. Актуальні кіберзагрози 2019 року

Тоді ж в травні ще одна шкідлива кампанія, яка поширювалася через Facebook, була виявлена експертами Radware3. Фішингові посилання відправлялися від заражених раніше осіб і вели на фальшиву сторінку YouTube, де жертві пропонувалося встановити розширення для браузера Google Chrome . Шкідливі розширення маскувалися під легітимні в офіційному каталозі Chrome Web Store, а на ділі перетворювали заражений комп'ютер в нову ланку ботнету: викрадали облікові дані користувачів в Facebook і Instagram, а потім продовжували поширення зловмисних програм серед друзів жертви (рис. 2). При цьому потужності заражених пристроїв використовувалися для майнінгу криптовалюти.

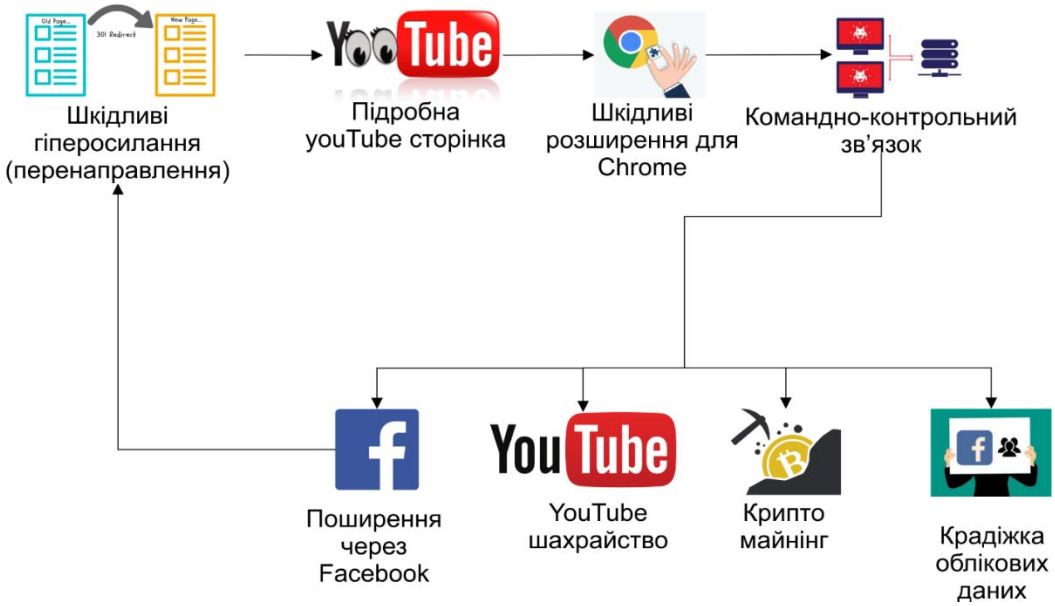

Рис. 2. Схема фішингу через Facebook.

Отже, фішинг може приймати різні форми і може бути досягнутий за допомогою безлічі інструментів і методів. Найбільш поширеними інструментами і методами, які використовуються для проведення фішингових атак є:

– Використання піддоменів.

Для нетехнічних користувачів, які не знайомі з ієрархією піддоменів, цей трюк працює як магія для хакера. Наприклад, електронний лист від відомого банку xyz, який запитує облікові дані користувача і просить перейти за URL-адресою www.xyzbank.user.com. Більшість користувачів буде вважати, що посилання буде перенаправляти в розділ xyz bank. Насправді, посилання перенаправить в розділ «xyzbank» на сайті www.user.com. Хоча домени унікальні, піддоменів немає, і, отже,

жоден власник домену не може заборонити будь-кому використовувати своє ім'я в якості піддомена свого домену. Ієрархія URL-адрес завжди йде справа наліво. Посилання mail.yahoo.com перенаправляє користувача на домен yahoo з піддоменів в якості пошти, тоді як yahoo.mail.com приводить до домену mail.com з субдоменів як yahoo.

– Приховані URL-адреси.

Інший широко використовуваний метод маніпулювання посиланнями - це коли зловмисник приховує фактичний URL-адресу під відкритим текстом. Це означає, що замість відображення фактичного URL злочинці використовують такі пропозиції, як «Натисніть тут» або «Підписатися». Насправді URL, що ховається за текстом, переводить користувачів до фішингових сайтів. Більш переконливий лист може навіть відображати фактичну посилання, наприклад, www.americanexpress.com, але якщо користувач натиснете на посилання, це приведе його до іншого веб-сайту. Іншим способом приховування URL-адреси є використання інструменту скорочення, наприклад tinyurl або bit.ly.

– Помилкові URL-адреси.

Іншим поширеним способом маніпулювання з посиланнями є те, що зловмисники будуть купувати домени з варіаціями в написанні популярного домена, наприклад, facebok.com, googlle.com, yahooo.com і т. і. Потім вони ошукують користувачів, створюючи схожі сайти і запитуючи особисту інформацію. Цей метод також відомий як викрадення URL або typosquatting. Перевага, яку отримує зловмисник, полягає в тому, що їх навіть не потрібно відправляти по електронній пошті, щоб отримати доступ. Швидше, невелика недбалість при наборі тексту може привести багатьох користувачів до них.

– Омографічні помилки.

У цьому методі зловмисник вводить користувача в оману, використовуючи в написанні схожі символи. Наприклад, користувач, який часто відвідує Citibank.com, може бути перенаправлений за посиланням, в якому Latin C замінюється кирилицею С. Крім того, символи, які здаються схожими, також можуть використовуватися для введння в обману. Наприклад, велика літера і (I) і маленька L (l), обидва виглядають однаково. Аналогічно, нуль (0) і велика о (O) також виглядають однаково.

– Підробка сайту.

Підробка сайту - це ще один метод фішингу, в результаті якого створюється сайт двійник для викрадення логінів і паролів. Веб-підроблення в основному здійснюється двома способами: міжсайтовий скриптинг і веб-спуфинг.

– Міжсайтовий скриптинг

Міжсайтовий скриптинг або XSS - це атака, в якій зловмисник використовує шкідливий скрипт у веб-додатоку або веб-сайті. Це дуже поширена і широко використовувана техніка, в якій використовується уразливість веб-додатків та веб-сайтів, який відвідує користувач. Зрештою, шкідливий скрипт попадає в браузер жертви.

Хоча злочинці можуть використовувати XSS в ActiveX або VBScript, найбільш поширеним є JavaScript, перш за все тому, що він використовується більшістю веб-сайтів сьогодення. Щоб змусити його працювати, зловмиснику потрібно буде ввести шкідливу надбудову на сторінку, яку відвідує жертва. Для того, щоб потенційна жертва відвідала сторінку, зловмисник використовує методи соціальної інженерії або маніпуляції посиланнями. Щоб зробити його більш успішним для зловмисника, використовується форма для введення особистих даних безпосередньо на сторінці підробленого сайту. Після цього зловмисник вставляє код, який буде використовуватися на веб-сторінці, і обробляється браузером користувача. Коли браузер завантажує сторінку, шкідливий скрипт виконується без будь яких дій з боку жертви, в більшості випадків користівач навіть не здогадується, що така атака сталася.

Захист від XSS можлива, хоча її неможливо повністю уникнути. Деякі браузери мають вбудований захист XSS, тому завжди рекомендується перевіряти параметри безпеки браузера і оновлювати браузери до останніх версій. Деякі надбудови, такі як NoScript для Firefox, дозволяють дозволити або заборонити використання скриптів.

– Spoofing сайту

Інший метод, який використовується для вебпідробки - веб-спуфинг, здійснюється шляхом створення фальшивого веб-сайту, який схожий на оригінальний веб-сайт, який користувач фактично має намір відвідати. Spoof сайт має аналогічний інтерфейс і дизайн і часто має схожий URL. Якщо користувач поспішаєте і не приділяєте багато уваги, то можете легко стати жертвою таких сайтів, які виглядають ідентично їх законним версіями.

– Вспливаючі вікна

Спливаючі повідомлення - один з найпростіших способів проведення успішних фішингових атак. Вони дозволяють зловмисникам викрадати реєстраційні дані, відправляючи користувачам спливаючі повідомлення і в кінцевому результаті переводять їх до підроблених веб-сайтів.

Ще один широко поширений метод фішинг-шахрайства - це «спливаюча технічна підтримка». При перегляді веб-ресурсів користувачі отримує спливаюче повідомлення про зараження системи, і необхідно звернутися до постачальника за технічною підтримкою.

Аналіз основного інструментарію фішингу, який був нами проведений, дав нам підстави сформулювати наступні рекомендації для організацій та підприємств стосовно захисту від фішингових атак:

1) Використання ефективних технічних засобів захисту:

– засоби централізованого управління оновленнями для використовуваного ПЗ;

– антивірусні програми (на всіх пристроях), в тому числі спеціалізовані, які, наприклад дозволяють користувачам відправляти підозрілі файли на перевірку перед відкриттям вкладення з листа;

– SIEM-рішення - для своєчасного виявлення атаки, якщо інфраструктура виявилась зараженою;

– автоматизовані засоби аналізу захищеності і виявлення вразливостей в ПЗ;

– мережевий екран рівня додатків (web application firewall) як превентивний захід захисту веб-ресурсів.

2) Захист даних:

– збереження конфіденційної інформації у закритому вигляді з обмеженим доступом;

– регулярне створення резервних копії систем і збереження їх на виділених серверах окремо від мережевих сегментів робочих систем;

– мінімізація привілеїв користувачів і служб;

– використання різних облікових записів і паролів для доступу до різних ресурсів;

– застосування двухфакторної аутентифікації там, де це можливо, наприклад для захисту привілейованих облікових записів.

– парольна політика, що передбачає суворі вимоги до мінімальної довжині і складності паролів;

– обмеження термінів використання паролів (не більше 90 днів).

3) Безпека персоналу:

– підвищення обізнаності працівників в питаннях ІБ;

– регулярне навчання персоналу правилам безпечної роботи в інтернеті,

– пояснення методів атак і способів захисту;

– застереження користувачів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої інформації кому б то не було по електронній пошті або під час телефонної розмови.

– пояснення порядку дій в разі підозр про шахрайство.

Висновки. Отже, для того, щоб запобігти або зменшити ймовірність настання фішингової атаки необхідно вжити перераховані вище заходи. Це не вичерпний перелік можливих дій, але це той мінімальний набір, який допоможе унеможливити реалізацію значної частини інструментарію соціальної інженерії.

ЛІТЕРАТУРА

[1]. А. Камалян, С. Кульов, К. Назаренко, *Комп'ютерні мережі та засоби захисту інформації: навчальний посібник*, Воронеж: (ВДАУ), 2003, 119 с

[2]. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. Режим доступу: http://zakon1.rada.gov.ua.

[3]. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. - Режим доступу: http:// zakon5. rada. gov. ua/ laws/ show/ 1126-97-%D0%BF.

[4]. А. Корченко, Е. Иванченко, С. Казмирчук, "Анализ и определение понятия риска для его интерпретации в области информационной безопасности", *Защита информации*, №3, 2010.

[5]. О. Корченко, *Системи захисту інформації: Монографія*, К.: НАУ, 2004, 264 с.

[6]. М. Тардаскін, *Технічний захист комерційної таємниці підприємства зв'язку: навч. посіб.*; за ред. М.В. Захарченко, М.Ф. Тардаскін, В.Г. Кононович, Одеса: ОНАЗ, 2002, 76 с.

[7]. Тотальна війна і комп'ютерний soft, як її головний інструмент. [Електронний ресурс]. Режим доступу: https://zillya.ua/totalna-viina-i-kompyuterniisoft-yak-golovnii-instrument

[8]. Фішинг: що це таке і як себе убезпечити? [Електронний ресурс]. Режим доступу: https://zillya.ua/fishing-shcho-tse-take-i-yak-sebe-ubezpechiti.

[9]. Фішинг: як не стати жертвою шахрайського сайту. [Електронний ресурс]. Режим доступу: https://gazeta.ua/articles/ema/_fishing-yak-ne-stati-zhertvoyu-shahrajskogo-sajtu/750605.

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ ВЛИЯНИЯ И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ФИШИНГУ

В статье проанализированы актуальные угрозы информационной безопасности и сделан прогноз основных направлений проведения кибератак в будущем. Выяснено, что среди существующих угроз информационной безопасности уже который год подряд первые позиции занимают методы социальной инженерии. Выделены наиболее распространенные инструменты и методы одной из составляющих социальной инженерии - фишинга, в частности всплывающие окна, межсайтовый скриптинг, ошибки URL-адреса и тому подобное. Исследователями сформулирован ряд рекомендаций по защите организаций и предприятий в контексте использования эффективных технических средств защиты (например, SIEM-решения - для своевременного обнаружения атаки, если инфраструктура оказалась зараженной, автоматизированные средства анализа защищенности и обнаружения уязвимостей в ПО, сетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты веб-ресурсов), непосредственной защиты данных (в частности, сохранение конфиденциальной информации в закрытом виде с ограниченным доступом, регуля не создание резервных копии систем и сохранения их на выделенных серверах отдельно от сетевых сегментов рабочих систем), а также безопасности персонала (в частности, повышение осведомленности работников в вопросах ИБ, регулярное обучение персонала правилам безопасной работы в Интернете, объяснения методов атак и способов защиты и т.п.).

Ключевые слова: Информационная безопасность, социальная инженерия, фишинг, средства защиты информации.

RESEARCH OF INFLUENCE TECHNOLOGIES AND METHODS OF COUNTERING FISHING

An increasing number of information security attacks that have occurred in the last year could have been prevented. Digitalization continues to be one of the main trends in modern business, which entails the use of both proven and latest information technologies in all sectors. Information security experts around the world are continuously fighting cybercrime. This makes the attackers perfect their tools. At the beginning of last year, cyber attacks became a test for many organizations in various sectors of the economy. Many events in the field of information security could be prevented. The large-scale and fast digitalization of all spheres of life and business that we are currently observing is based on the use of a mass of information technologies (both already proven and credible, as well as the latest). However, as practice shows, even security technologies that have been used for years have not been resolved. A cyber attack on a company with a well-organized defense system requires special knowledge and tools, as well as high financial and time costs. Multistage, carefully planned and organized cyber attacks aimed at a specific industry or specific, usually large, companies are called advanced persistent threats. The article analyzes the current threats to information security and makes a forecast of the main directions of cyber attacks in the future. Among the existing threats to information security, for several consecutive years, the leading position has been occupied by methods of social engineering. Cybercriminals continue to invent new methods of influencing users that would allow them to infect the target system with malware, steal money or gain access to confidential information. Phishing can take many forms and can be achieved using a variety of tools and techniques. During the analysis, the authors identified the most common tools and methods that are used to conduct phishing attacks. The analysis made it possible to formulate the necessary measures in order to reduce the number of successful phishing attacks. This is not an exhaustive list of possible actions, but a minimal set that will make it impossible to implement much of the social engineering toolkit.

Keywords: information security, social engineering, phishing, information security tools.

Мехед Дмитро Борисович, к.п.н., доцент кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: d.mekhed@gmail.com.
Orcid ID: 0000-0003-3905-3620.
Мехед Дмитрий Борисович, к.п.н., доцент кафедры кибербезопасности и математического моделирования Черниговского национального технологического университета.
Mekhed Dmytro, PhD, associate professor of the Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology.

Ткач Юлія Миколаївна, д.пед.н., доцент, завідувач кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.
E-mail: tkachym79@gmail.com.
Orcid ID: 0000-0002-8565-0525.
Ткач Юлия Николаевна, д.пед.н., доцент, заведующая кафедрой кибербезопасности и математического моделирования Черниговского национального технологического университета.
Tkach Yulia, Doctor of Pedagogical Science, associate professor, Head of the Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology.

Базилевич Володимир Маркович, к.е.н., зав. кафедри інформаційних та комп'ютерних систем Чернігівського національного технологічного університету.
E-mail: bazvlamar@gmail.com.
Orcid ID: 0000-0001-8935-446X.
Базилевич Владимир Маркович, к.е.н., зав. кафедры информационных и компьютерных систем Черниговского национального технологического университета.
Bazylevych Volodymyr, PhD, associate professor of information and computer system department, Chernihiv National University of Technology.