http://ma123.ru **ЦИТИСЭ** № 1 (43) 2025 **ISSN** 2409-7616

Научная статья
УДК 37.01:007

ВЛИЯНИЕ ИНТЕРАКТИВНЫХ ТРЕНИНГОВ НА ОСВЕДОМЛЕННОСТЬ СОТРУДНИКОВ О ФИШИНГОВЫХ АТАКАХ

Д.С. Ан, А.С. Зуфарова

Ан Дмитрий Станиславович,
студент, Тихоокеанский государственный университет, Хабаровск, Россия.
2019100305@pnu.edu.ru

Зуфарова Анна Сергеевна,
старший преподаватель кафедры математических методов защиты информации и компьютерной безопасности, Тихоокеанский государственный университет, Хабаровск, Россия.
006694@pnu.edu.ru

Аннотация. *В современном мире информационные технологии занимают центральное место в деятельности организаций, государств и частных лиц. Цифровая трансформация бизнеса и широкое распространение интернета привели к тому, что информация стала одним из самых ценных ресурсов. Однако с ростом зависимости от технологий также увеличивается количество угроз, связанных с кибербезопасностью. Одной из наиболее опасных и распространенных угроз является социальная инженерия. Социальная инженерия остаётся одной из главных угроз в мире кибербезопасности благодаря своей гибкости и способности обходить технические меры защиты. Подделка голоса, образы людей, монтаж и создание фейковых видео, аренда колл-центров с операторами-мошенниками, звонки якобы от спецслужб или банков, использование искусственного интеллекта, фишинговые SaaS-сервисы — это лишь малая часть современных инструментов мошенников, которые взламывают не системы защиты или машины, а самого человека. Фишинг — самая распространенная и успешная форма кибермошенничества в современном обществе. В условиях постоянного роста технологий, таких как онлайн-сервисы и компьютерные и мобильные приложения, методы фишинга становятся всё более непредсказуемыми и неожиданными для общества. Все эти факты подчеркивают значимость проблемы и выявляют необходимость в эффективных методах борьбы с фишингом. Понимание различных видов социальной инженерии и обучение сотрудников правилам безопасного поведения помогают снизить риски успешных атак. Интерактивные тренинги по осведомлённости о фишинговых атаках играют ключевую роль в повышении уровня кибербезопасности в организациях. Такие тренинги помогают сотрудникам распознавать и избегать фишинга, что способствует снижению рисков и повышению общей культуры безопасности. В данной статье рассматривается влияние интерактивных тренингов на осведомленность сотрудников и их эффективность в обучении навыкам безопасного поведения при работе с электронными письмами.*

http://ma123.ru **ЦИТИСЭ** № 1 (43) 2025 **ISSN** 2409-7616

Ключевые слова: *социальная инженерия, фишинг, интерактивный тренинг, обучение, безопасность, e-mail рассылки, результат, защита информации.*

Библиографическая ссылка: *Ан Д.С., Зуфарова А.С. Влияние интерактивных тренингов на осведомленность сотрудников о фишинговых атаках // ЦИТИСЭ. 2025. № 1. С. 41-52.*

Research Full Article
UDC 37.01:007

THE IMPACT OF INTERACTIVE TRAINING ON AWARENESS INFORMATION ABOUT PHISHING ATTACKS

D.S. An, A.S. Zufarova

Dmitry S. An,
Student, Pacific State University, Khabarovsk,
Russian Federation.
2019100305@pnu.edu.ru

Anna S. Zufarova,
Senior Lecturer at the Department Mathematical Methods of Information Security and Computer Security, Pacific State University, Khabarovsk,
Russian Federation.
006694@pnu.edu.ru

Abstract. *In the modern world, information technology occupies a central place in the activities of organizations, states and individuals. The digital transformation of business and the widespread use of the Internet have led to the fact that information has become one of the most valuable resources. However, with increasing dependence on technology, the number of threats related to cybersecurity is also increasing. One of the most dangerous and widespread threats is social engineering. Social engineering remains one of the main threats in the world of cybersecurity due to its flexibility and ability to circumvent technical protection measures. Voice forgery, human image, installation and creation of fake videos, leased call centers with fraudulent operators, calls from special services or a bank, the use of artificial intelligence, phishing SaaS services are only a small part of modern fraudsters' tools that hack the person himself, not security systems or machines. Phishing is the most common and successful form of cyberbullying in modern society. In the context of constantly growing technologies: online services, computer applications and mobile phishing methods are becoming more unpredictable and unexpected for society. All these facts emphasize the importance of the problem and reveal the need for effective methods to combat phishing. Understanding various types of social engineering and training employees in safe behavior rules help reduce the risks of successful attacks. Interactive phishing awareness training plays a key role in improving cybersecurity in organizations. These trainings help employees recognize and avoid phishing, which helps reduce risks and enhance the overall security culture. This article examines the impact of interactive trainings on employee awareness and their effectiveness in teaching the skill of safe behavior with emails.*

Keywords: *social engineering, phishing, interactive training, education, security, e-mail newsletters, result, information protection.*

For citation: *An D.S., Zufarova A.S. The impact of interactive training on awareness information about phishing attacks. CITISE, 2025, no. 1, pp. 41-52.*

Введение.

В современном мире, где информационные технологии стремительно развиваются, а киберугрозы становятся все более опасными и изощрёнными. Вопрос об обеспечении информационной безопасности в обществе приобретает особую актуальную роль. Любая организация хранит оцифрованную информацию, имеет выход в глобальную сеть интернет и уязвима перед киберпреступниками. Одной из наиболее распространенных и опасных форм кибератак являются социальная инженерия, а именно фишинговые атаки. С ними сталкиваются не только простые пользователи интернета, но и даже объектов критической информационной инфраструктуры (КИИ).

В 2023 году хакеры с помощью фишинга взломали сотрудников авиакомпании и туроператора. Преступники создали авиабилетов на 2 млн долларов. Так же в 2017 году атака с помощью фишинга произошла на военно-промышленный комплекс России. В 2020 году по данным Group-IB хакеры из КНДР атаковали российские оборонные предприятия. Атака произошла через фишинговое письмо. Так же в 2021 был атакован с помощью целевого фишинга АО «Государственный ракетный центр имени академика В. П. Макеева». В апреле 2024 года масштабной атаке подвергся Агрокомплекс им. Н.И. Ткачева, одна из причин взлома фишинг [5]. И это еще не все случаи, где причиной взлома было электронное письмо.

Получается никто не застрахован от этой атаки: ни простой пользователь и ни крупная компания со всеми возможными системами безопасностями. Возглавляет пирамиду безопасности — человек, а он уязвим.

Основная часть.

В последнее время социальная инженерия привлекает внимание не только специалистов по информационной безопасности, но и по психологии. Одним из известных исследователей в области социальной инженерии является Кевин Митник, бывший хакер и ныне консультант по информационной безопасности. В своих книгах «Искусство обмана» («The Art of Deception») и «Искусство вторжения» («The Art of Intrusion») он подробно описывает используемые психологические манипуляции [1, 2]. Еще одна важная работа — книга «Ловушки мышления. Почему разум ошибается в условиях опасности», автором которой является Брюс Шнайер, специалист по кибербезопасности. В ней автор акцентирует внимание на проблеме доверия и уязвимостях человеческого поведения. Книга «Социальная инженерия: искусство хакерских атак» Кристофера Хэндегги предлагает практические рекомендации по предотвращению манипуляций в корпоративной среде. В 2007 году была издана книга Максима Кузнецова и Игоря Симдянова «Социальная инженерия и социальные хакеры», ставшая первой известной работой по социальной инженерии в контексте информационной безопасности в России.

Исследования в этой области продолжают развиваться и в научном сообществе. Например, Джессика Баркер в своем труде «Cybersecurity ABCs: Delivering Awareness, Behaviors, and Culture» исследует человеческие аспекты информационной безопасности. Она анализирует пути формирования информационной культуры и то, как осведомленность и поведение человека в стрессовых ситуациях могут противостоять атакам социальной инженерии. Исследования, публикации книг и научные статьи в области социальной инженерии указывают на важность формирования информационной культуры и правильного поведения

пользователей в виртуальном пространстве, а также на необходимость повышения осведомленности сотрудников для снижения риска атак [6].

Актуальность темы обусловлена тем, что многие сотрудники не обладают достаточными знаниями и навыками для распознавания фишинговых атак. Социальная инженерия в информационной безопасности — это совокупность методов обмана человека с целью побудить его к действиям, способствующим несанкционированному доступу к информации или инфраструктуре [12].

Теперь обратимся к определению фишинга. Фишинг (англ. phishing, от fishing — рыбная ловля) — это одна из самых распространенных форм социальной инженерии, включающая рассылку поддельных электронных писем, сообщений или создание фальшивых веб-сайтов с целью заставить пользователя раскрыть свои личные данные (логины, пароли, номера кредитных карт и т. п.). Среди наиболее распространенных видов фишинга можно выделить массовую рассылку (стандартный фишинг через электронную почту), дипфейковый фишинг, мобильный фишинг (смс-фишинг), смишинг, вишинг, целевой фишинг, фишинг через социальные сети, форумы или объявления, фишинг с использованием QR-кодов и многое другое. Цель этих атак — обман пользователей с целью получения конфиденциальной информации: паролей, номеров кредитных карт, личных данных и других интересующих злоумышленника сведений. Кроме того, благодаря таким атакам можно получить доступ к данным крупных и значимых предприятий, особенно в наше время. Фишинг представляет собой угрозу не только для обычных пользователей глобальной сети, но и для любых организаций. Несмотря на наличие технической защиты, человек часто оказывается причиной 74% инцидентов безопасности в 2024 году [1; 7]. Статистика показывает, что большинство успешных взломов происходят именно через фишинг, так как злоумышленники эксплуатируют человеческие слабости, такие как невнимательность и недостаточная осведомленность.

Известны следующие цитаты компаний, работающих в сфере информационных технологий: «Ключевыми способами проникновения злоумышленников в инфраструктуру остаются фишинг и социальная инженерия, то есть человеческий фактор» («Ростелеком-Solar») [1]. «... Какими бы ни были технологии, они теряют смысл, если сотрудники открывают подозрительные файлы и кликают на фишинговые ссылки...» (Group-IB) [1].

А вот что сообщает «Интерфакс» со ссылкой на заместителя председателя правления Сбербанка: «... Сейчас в России около 30% офисов...А вот что об этом пишет «Интерфакс» со ссылкой на зампреда правления Сбербанка: «... сейчас в России больше 30% офисных работников имеют склонность открывать фишинговые письма. Этот тренд сохраняется с ростом 1-2% примерно за квартал. В целом потери российской экономики в 2019 г. от действий кибератак оцениваются в 2,5 трлн рублей» [1].

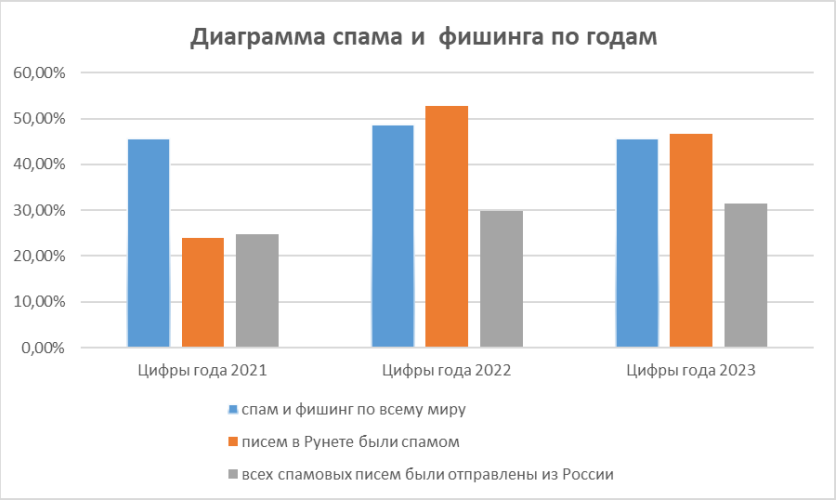

Рисунок 1 — Диаграмма спама и фишинга по годам

Мы проанализировали отчеты компании Kaspersky по спаму и фишингу за 2021, 2022 и 2023 годы [11].

На рисунке 1 представлена диаграмма спама и фишинга по годам. Первое, что видно: как спам и фишинг по всему миру растут и не спадают. Растёт количество писем в рунете в виде спама. Также выявлена растущая тенденция отправленных фишинговых писем из страны России.

На диаграмме фишинга в электронной почте (рисунок 2) видно, динамику системы «Антифишинг». С 2021 по 2023 происходит рост распространение фишинговых ссылок в электронных письмах [9].

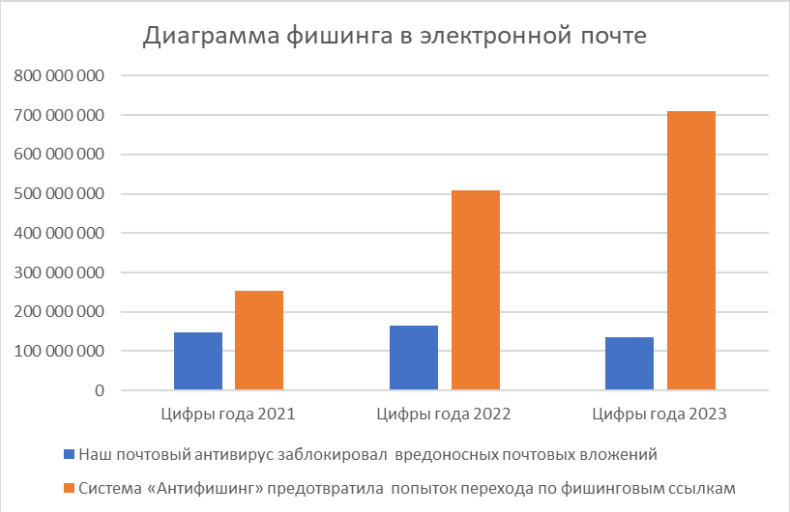

Рисунок 2 — Диаграмма фишинга в электронной почте по годам

На диаграмме фишинга в мессенджеров (рисунок 3), выявлено рост распространения фишинговых ссылок через телефонные мессенджеры (WhatsApp, Viber, Telegram). Это связано с переходом на дистанционную работу и учебу в период Covid 19. С популярностью Telegram выявлены попытки перехода по фишинговым ссылка, чтобы взломать и украсть аккаунты Telegram для дальнейшего использование в корыстных целях [8].

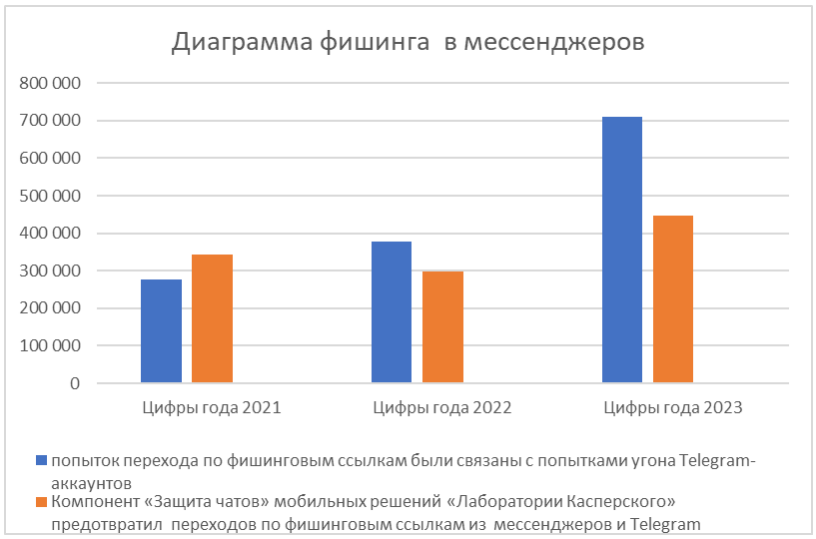

Рисунок 3 — Диаграмма фишинга в мессенджерах по годам

В рамках нашего исследования, был создан опрос по социальной инженерии: «Распознания разновидности фишинга». В нем участвовали люди разных возрастов, профессий, компетенций и пола. В исследование охватили все возрастные диапазоны от подростков до старшего поколения. Участвовало 110 человек. Выяснили, что почти 80% опрошенных людей сталкивались с мошенниками (рис. 4). Многие попадались на их уловки, что в итоге теряли свои финансы, личную информацию и другое.

Рисунок 4 — Результат опроса «Попадались ли вы на уловки мошенников»

Так же почти половина, знакома с такими понятиями: социальная инженерия, фишинг, дипфейк-фишинг, фарминг и другое. Но почти 30 % не знакомы с такими понятия,
то есть не осведомлены (рис. 5).

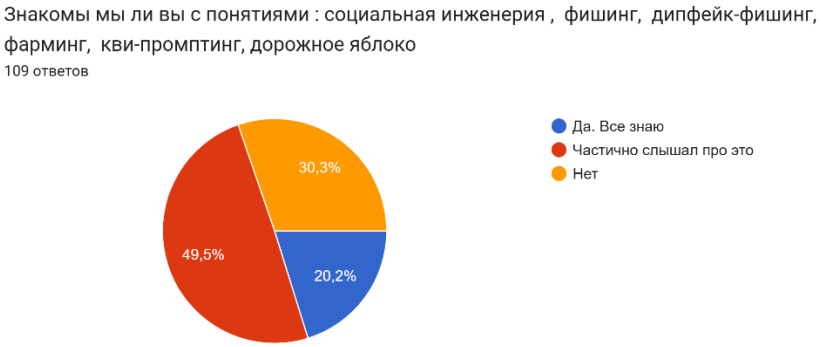

Рисунок 5 — Результат опроса о знаниях фишинга

Так же испытуемые прошли входное тестирование на знания фишинга. Самый минимальный результат был 4 балла из 19 и максимальный 15 из 19. В среднем результат показал 12 баллов из 19. Результаты представлены на рисунке 6.

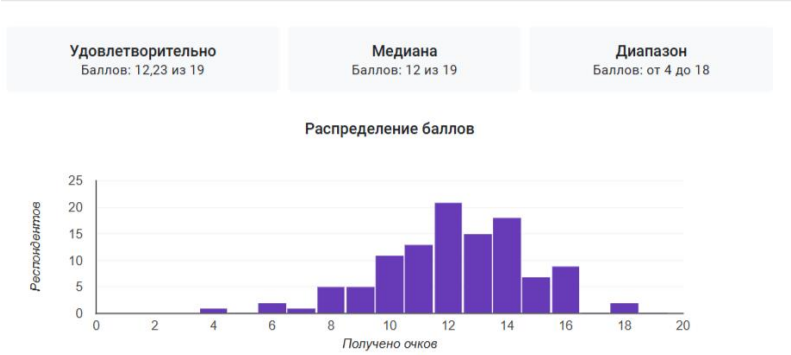

Рисунок 6 - Результаты тестирования

По результатам исследования видно, что не все пользователи компетентны в вопросах социальной инженерии — фишинг. В связи с этим обучение сотрудников методам защиты от фишинга становится неотъемлемой частью стратегии обеспечения безопасности на любом предприятии. Также надо ввести уроки в школах, гимназиях, техникумах, вузах предмет «информационная гигиена», где ребята будут узнавать новое об информационной безопасности.

Исследования показывают, что именно человеческий фактор зачастую становится слабым звеном в системе безопасности. Поэтому разработка эффективной стратегии для обучения сотрудников по «определению фишинга» является важной задачей, способствующей повышению общего уровня информационной безопасности на предприятиях. Обучение сотрудников является ключевым элементом защиты от атак фишинга. Оно должно включать: регулярные тренинги, симуляцию фишинговых атак, инструкции противодействий. Основные цели антифишинговых учений — это обучить пользователей распознавать фишинговые атаки, сообщать о них и избегать их, что поможет защитить их и отдел от киберугроз. Помочь службе ИБ собирать более качественные показатели и информацию об атаках с использованием электронной почты, чтобы лучше защитить сеть от этих угроз.

Одним из эффективных способов достижения этой цели являются интерактивные тренинги.

Интерактивный тренинг – это форма обучения, которая активно вовлекает участников в учебный процесс через взаимодействие с тренером, другими участниками и учебными материалами.

Цель интерактивного тренинга заключается в том, чтобы сделать обучение более динамичным, интересным и эффективным за счет активного участия обучающихся [14].

Интерактивные тренинги отличаются от традиционных лекций и семинаров тем, что они вовлекают участников в активный процесс обучения. Вместо пассивного прослушивания материала сотрудники участвуют в практических заданиях, имитирующих реальные фишинговые сценарии. Это позволяет им не только узнать теоретические основы, но и применить полученные знания на практике [15].

В инфографике (рисунок 7) представлены основные характеристики интерактивного тренинга: активное участие, геймификация, обратная связь, практическая направленность, диалог и обсуждение, мультимедийные элементы.

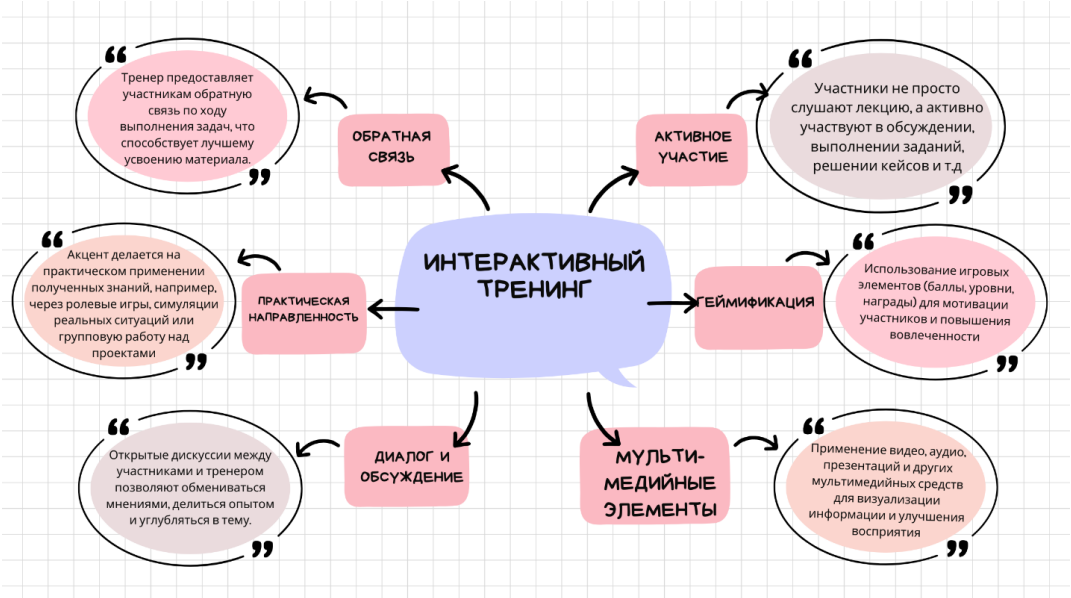

Рисунок 7 - Инфографика интерактивного треннинга

В следующей инфографике (рисунок 8) представлены «Преимущества интерактивных тренингов»: возможность применения новых технологий, усвоение и запоминание материала, коммуникативные навыки, индивидуальный подход, гибкость формата и повышение мотивации [16; 17].

Рисунок 8 - Инфографика Преимущества интерактивных тренингов в обучении фишинга

Рассмотрим подходящие виды интерактивных тренингов для повышения осведомленности о фишинге [10].

Первый вид — это симулированные фишинг кампании. Их проводят внутри компании с помощью специально разработанного программного обеспечения по обучению фишинга или составлено вручную отделом безопасности. Сотрудники получают электронные письма или сообщения, которые внешне похожи на настоящие фишинговые, но на самом деле созданы безопасными средствами. Целью таких кампаний является выявление уязвимых мест и оценка готовности сотрудников противостоять реальным угрозам [18].

Следующий это онлайн-курсы, тесты, викторины. Участники проходят мини разделы посвященные фишингу. После освоения курсов, участники проверяют свои знания с мощью тестов или вопросов. Такой формат удобен для дистанционного обучения и позволяет сотрудникам учиться в удобное для них время.

В эти онлайн -курсы можно включить игры, симуляции, виртуальную реальность.

Эти интерактивные компоненты, позволяют участникам погружаться в вымышленные сценарии, где они должны принимать решения и действовать в условиях, напоминающих реальную жизнь. Это не только интересно, но и эффективно, так как стимулирует активное участие и запоминание информации. Так же внутри компании можно организовать мастер-классы, тренинги и воркшопы. Они проводятся экспертами в области кибербезопасности и фокусируются на практическом применении знаний. Участникам предлагаются конкретные кейсы и задачи, которые нужно решить коллективно или индивидуально.

Мы отобрали группу людей участвующих 15 человек [19]. Провели входное тестирование. Получили результат, представлены на рисунке 10 Тест 1.

На втором этапе, нами был проведен викторина «Безопасный интернет. Основы фишинга» в виде игры. Где обучающаяся в форме игры познали для себя актуальные и интересные факты о безопасном интернете и фишинге.

Так же на практическом занятие было предложено задание «Создание собственного фишинга». Такой вид работы развивает критическое мышление и понимание того, как работают фишинговые схемы. Участники поделились на группы составителей и проверяющих. Первая команда создавала собственные «фишинговые» письма, а вторая попыталась выявить признаки мошенничества в этих письмах.

На заключающем этапе, было проведено итоговое тестирование по знанию и распознанию фишинга. Результаты представлены на рисунке 9 Тест 2. Результат почти у всех участников улучшился.

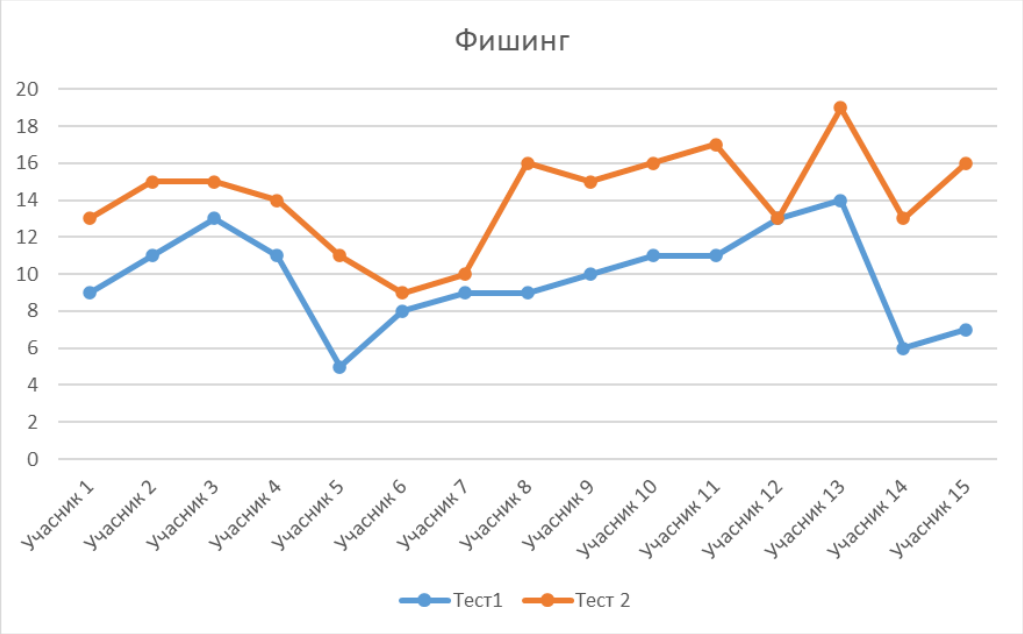

Рисунок 9 - Результат эксперимента

Вывод.

Социальная инженерия остаётся одной из главных угроз в мире кибербезопасности благодаря своей гибкости и способности обходить технические меры защиты. Понимание различных видов социальной инженерии и обучение сотрудников правилам безопасного поведения помогают снизить риски успешных атак. Однако, учитывая постоянное развитие технологий и методов социальной инженерии, необходимо регулярно обновлять стратегии защиты и проводить обучение персонала. Интерактивные тренинги представляют собой один из эффективных способов обучения и распознавания фишинговых атак.

Интерактивные тренинги играют важную роль в повышении осведомленности сотрудников о фишинговых атаках. Они позволяют участникам не только узнать теорию, но и применить её на практике, что значительно увеличивает шансы на успешное противостояние реальным угрозам. Компании, которые инвестируют в такие тренинги, не только защищают свои данные, но и создают культуру безопасности, в которой каждый сотрудник осознаёт свою ответственность за защиту информации.

Исследования показывают, что интерактивные тренинги действительно повышают уровень осведомлённости сотрудников о фишинге. Например, одно исследование, проведённое компанией Proofpoint, показало, что после прохождения интерактивных курсов число сотрудников, попадающихся на фишинг, снизилось на 40% [13]. Кроме того, сотрудники стали чаще сообщать о подозрительных письмах и сообщениях, что помогло предотвратить потенциальные утечки данных.

Таким образом, интерактивные тренинги являются мощным инструментом в борьбе с фишингом и другими видами социальной инженерии. Регулярное проведение таких тренингов

помогает поддерживать высокий уровень осведомлённости и готовности сотрудников к возможным угрозам, что существенно укрепляет общую безопасность организации.

Список источников:

1. Другач Ю. С. Контролируемый взлом. Библия социальной инженерии. - 2-е изд., перераб. и доп. - СПб.: БХВ-Петербург, 2024. - 208 с.
2. Иванов П.И. Противодействие фишинговым атакам: обучение пользователей безопасности. М.: Наука, 2020. 256 с.
3. Ефимов С.А., Пронькин Н.Н. Роль сотрудников в обеспечении информационной безопасности: подходы к повышению осведомлённости // International Journal of Professional Science. 2024. № 6-2. С. 40-47. URL: https://elibrary.ru/evqrjk
4. Прохоров А. И. Фишинг-атаки: основные виды и способы защиты от них / А. И. Прохоров, Е. А. Маркин, У. Г. Никеева // Информационные системы, экономика и управление: Ученые записки. – Ростов-на-Дону: Ростовский государственный экономический университет (РИНХ, 2023. С. 84-90. URL: https://elibrary.ru/mzgipc
5. Бачиева А.В. Фишинг как один из способов мошенничества в сфере компьютерной информации / А. В. Бачиева, Т. О. Бозиев // Актуальные проблемы юридической науки и практики. Том 1. - Гатчина: Государственный институт экономики, финансов, права и технологий, 2017. - С. 232-235. URL: https://www.elibrary.ru/zhtgzh
6. Васильева Н.А. Методы защиты сотрудников от фишинговых атак: роль тренингов и образования. - М.: РУДН, 2020. - 220 с.
7. Захарова А.А. Методы обучения персонала в организации // Аллея науки. 2022. Т. 1, № 3 (66). С. 114-120. URL: https://www.elibrary.ru/acjlnb
8. Абитов А.А. Защита от фишинга / А. А. Абитов, Р. А. Тхакахов, М. З. Хачмахова, К. Ш. Сунгуров // Цифровая трансформация науки и образования: Сборник научных трудов. Часть III. - Нальчик: Кабардино-Балкарский государственный университет им. Х.М. Бербекова, 2020. - С. 13-17. URL: https://www.elibrary.ru/xcbynd
9. Вилкова А.В., Литвишков В.М., Швырев Б.А. Встроенное обучение как элемент непрерывного обучения информационной безопасности // Пенитенциарная наука. 2020. Т. 14. № 1 (49). С. 135-141. URL: https://www.elibrary.ru/xidpsr
10. Жданова Д.Е. Технология реверсивного обучения: сочетание мобильного обучения и активных методов обучения // Наукосфера. 2021. № 7-1. С. 55-58. URL: https://elibrary.ru/siqyud
11. Нечипуровский Д.И. Как построить многоуровневую защиту для борьбы с продвинутыми угрозами фишинга // Научный аспект. 2024. Т. 41, № 4. С. 5337-5342. URL: https://www.elibrary.ru/jdtfvy
12. Богданова Т.М. Повышение безопасности сотрудников через тренировки по фишинговым атакам. - М.: РАН, 2019. - 153 с.
13. Яковлева М.А. Лидерство в системе наставничества как эффективный инструмент адаптации персонала // Human Progress. 2021. Т. 7, № 1. 17. URL: https://www.elibrary.ru/mfmyrr
14. Штайгер А.А. Социальная инженерия на примере фишинга // Вестник современных исследований. 2018. № 6.3 (21). С. 612-614. URL: https://www.elibrary.ru/xuroqp
15. Зуфарова А.С., Кошелева А.Д. Формирование методики создания интерактивных образовательных web-квестов в условиях школьного образования // Современное педагогическое образование. 2024. № 6. С. 116-120. URL: https://www.elibrary.ru/tyomig
16. Павлов А.С. Методика оценки эффективности тренингов по фишингу в организациях. - М.: Высшая школа экономики, 2020. - 276 с.

17. Козлова О.В. Интерактивные методы обучения для повышения осведомленности о фишинговых атаках. - СПб.: Невский университет, 2019. - 162 с.

18. Климов А.А., Заречкин Е.Ю., Куприяновский В.П. Влияние цифровизации на систему профессионального образования // Современные информационные технологии и ИТ-образование. 2019. Т. 15, № 2. С. 468-476. URL: https://www.elibrary.ru/ixhcvv

19. Сливинский Д.В., Шишияну К.С. Обучение персонала как технология управления человеческими ресурсами предприятия: основные формы, методы и критические оценки // Инновации и инвестиции. 2023. № 11. С. 78-80. URL: https://www.elibrary.ru/bwijwi

References:

1. Drugach Y. S. *Controlled hacking. The Bible of Social Engineering.* 2nd ed., reprint. and additional. St. Petersburg, BHV-Petersburg Publ., 2024. 208 p. (In Russian).

2. Ivanov P.I. *Countering phishing attacks: training security users*. Moscow, Nauka Publ., 2020. 256 p (In Russian).

3. Efimov S.A., Pronkin N.N. The role of employees in ensuring information security: approaches to raising awareness. *International Journal of Professional Science*, 2024, no. 6-2, pp. 40-47. (In Russian). URL: https://elibrary.ru/evqrjk

4. Prokhorov A.I., Markin E.A., Nikeeva U.G. Phishing attacks: main types and methods of protection against them. Proc. *"Information systems, economics and management: Scientific notes"*. Rostov-on-Don, Rostov State University of Economics (RINH) Publ., 2023. pp. 84-90. URL: https://elibrary.ru/mzgipc

5. Bachieva A. V. T. O. Boziev Phishing as one of the methods of fraud in the field of computer information. Proc. "Actual problems of legal science and practice". Vol. 1. Gatchina, State Institute of Economics, Finance, Law and Technology Publ., 2017. pp. 232-235. URL: https://www.elibrary.ru/zhtgzh

6. Vasilyeva N.A. *Methods of protecting employees from phishing attacks: the role of training and education.* Moscow, RUDN Publ., 2020. 220 p. (In Russian)

7. Zakharova A.A. Methods of personnel training in the organization. *Alley of Science,* 2022, vol. 1. no. 3 (66), pp. 114-120. (In Russian). URL: https://www.elibrary.ru/acjlnb

8. Abitov A.A., Thakakhov R.A., Khachmakhova M.Z. et al. *Protection from phishing.* Proc. *"Digital transformation of science and education"*. Nalchik, Kabardino-Balkarian State University named after H.M. Berbekov Publ., 2020. pp. 13-17. (In Russian). URL: https://www.elibrary.ru/xcbynd

9. Vilkova A.V., Litvishkov V.M., Shvyrev B.A. Embedded learning as an element of continuous information security training. *Penitentiary Science*, 2020, vol. 14, no. 1 (49), pp. 135-141. (In Russian). URL: https://www.elibrary.ru/xidpsr

10. Zhdanova D.E. Technology of reverse learning: a combination of mobile learning and active learning methods. *Naukosphere,* 2021, no. 7-1, pp. 55-58. (In Russian). URL: https://elibrary.ru/siqyud

11. Nechipurovsky D.I. How to build a multi-level protection to combat advanced phishing threats. *Scientific aspect.* 2024. Vol. 41. No. 4. pp. 5337-5342. (In Russian). URL: https://www.elibrary.ru/jdtfvy

12. Bogdanova T.M. *Improving employee safety through training on phishing attacks*. Moscow, RAS Publ., 2019. 153 p. (In Russian).

13. Yakovleva M.A. Leadership in the mentoring system as an effective tool for personnel adaptation. *Human Progress*, 2021, vol. 7, no. 1. id. 17. (In Russian). URL: https://www.elibrary.ru/mfmyrr

14. Steiger A.A. Social engineering on the example of phishing. *Bulletin of Modern Research,* 2018, no. 6.3 (21), pp. 612-614. (In Russian). URL: https://www.elibrary.ru/xuroqp

15. Zufarova A.S., Kosheleva A.D. Formation of a methodology for creating interactive educational web-quests in the conditions of school education *Modern Pedagogical Education*, 2024, no. 6, pp. 116-120. (In Russian). URL: https://www.elibrary.ru/tyomig

16. Pavlov A.S. *Methodology for evaluating the effectiveness of phishing trainings in organizations.* Moscow, Higher School of Economics Publ., 2020. 276 p. (In Russian)

17. Kozlova O.V. *Interactive teaching methods to raise awareness of phishing attacks*. St. Petersburg, Nevsky University Publ., 2019. 162 p. (In Russian)

18. Klimov A.A., Zarechkin E.Yu., Kupriyanovsky V.P. The impact of digitalization on the vocational education system. *Modern information technologies and IT education*, 2019, vol. 15, no. 2, pp. 468-476. (In Russian). URL: https://www.elibrary.ru/ixhcvv

19. Slivinsky D.V., Shishiyanu K.S. Personnel training as a technology for managing human resources of an enterprise: basic forms, methods and critical assessments. *Innovations and investments*, 2023, no. 11, pp. 78-80. (In Russian). URL: https://www.elibrary.ru/bwijwi

Submitted: 01 December 2024 Accepted: 12 January 2025 Published: 14 January 2025