УДК 004.055

ЭВОЛЮЦИЯ МЕТОДОВ ФИШИНГА И СПОСОБЫ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНОЙ СРЕДЕ

Контанджян А.В.

к.э.н., доцент

Вятский государственный университет,

Киров, Россия

Валова Н.А.

студент 4 курса,

Вятский государственный университет,

Киров, Россия

Опарина Э.Н.

студент 4 курса,

Вятский государственный университет,

Киров, Россия

Прозорова С.С.

студент 4 курса,

Вятский государственный университет,

Киров, Россия

Аннотация

В статье исследуется проблема роста киберпреступности, в частности фишинговых атак, направленных на сотрудников корпоративной среды. На основе анализа статических данных и современных трендов рассмотрена эволюция методов фишинга: от примитивных массовых рассылок до высокотехнологичных атак с применением искусственного интеллекта и

технологий глубоких подделок. Охарактеризованы ключевые угрозы для бизнеса. Особое внимание уделено формированию комплексной стратегии защиты пользователей, основанной на трёх взаимосвязанных направлениях: системном обучении персонала и проведении фишинг-симуляций, внедрении технических средств контроля и оптимизации организационных процедур. Сделан вывод, что в условиях постоянной трансформации фишинговых угроз только многоуровневый подход, интегрирующий киберграмотность сотрудников, современные технологии и чёткие бизнес-процессы, обеспечивает устойчивую защиту корпоративной информационной среды.

Ключевые слова: фишинг, кибербезопасность, корпоративная среда, социальная инженерия, эволюция методов фишинга, защита пользователей, утечка данных, информационная безопасность.

EVOLUTION OF PHISHING TECHNIQUES AND USER PROTECTION IN THE CORPORATE ENVIRONMENT

Kontanjian A.V.
Candidate of Economic Sciences, Associate Professor
Vyatka State University,
Kirov, Russia

Valova N.A.
4th year student,
Vyatka State University,
Kirov, Russia

Oparina E.N.
4th year student,
Vyatka State University,

Kirov, Russia

Prozorova S.S.
4th year student,
Vyatka State University,
Kirov, Russia

Abstract

The article explores the problem of the growth of cybercrime, in particular, phishing attacks aimed at employees of the corporate environment. Based on the analysis of static data and modern trends, the evolution of phishing methods is considered: from primitive mass mailings to high-tech attacks using artificial intelligence and deep fake technologies. The key threats to business are characterized. Special attention is paid to the formation of a comprehensive user protection strategy based on three interrelated areas: systematic staff training and phishing simulations, implementation of technical means of control and optimization of organizational procedures. It is concluded that in the context of the constant transformation of phishing threats, only a multi-level approach that integrates employee cyber literacy, modern technologies, and clear business processes can provide sustainable protection for the corporate information environment.

Keywords: phishing, cybersecurity, corporate environment, social engineering, evolution of phishing methods, user protection, data leakage, and information security.

В результате развития современных цифровых технологий с каждым годом увеличивается число пользователей, ставших жертвами преступных проявлений, совершенных с использованием ИТ-технологий, причём каждое

седьмое преступление в нашей стране совершается с использованием именно данных технологий [4].

Согласно данным, представленным Министерством внутренних дел Российской Федерации по состоянию на февраль 2026 года, в течение 2025 года было зарегистрировано 663 тысячи киберпреступлений. Преобладающая часть из них, а именно более половины, приходится на преступления, связанные с мошенничеством. В подобной ситуации человек сам, осознавая свои действия, передаёт секретные сведения, которые впоследствии могут быть использованы злоумышленниками для причинения финансового ущерба. Зачастую такие данные добываются путём фишинга, представляющего собой разновидность онлайн-мошенничества.

Актуальность темы, обусловлена тем, что многие сотрудники предприятий, фирм и простые пользователи не обладают достаточными знаниями и навыками для распознавания фишинговых атак. А некоторые люди вообще не знакомы с понятием социальной инженерией - фишингом [2].

Фишинг - это вид мошенничества, при котором злоумышленники, притворяясь доверенными лицами или компаниями, обманом выманивают у жертв конфиденциальные данные (пароли, банковские реквизиты). Для этого они рассылают поддельные электронные письма, имитирующие сообщения от легальных организаций (банков, интернет-магазинов). Эти письма содержат ссылки, ведущие на фальшивые сайты, которые выглядят как настоящие. Мошенники используют психологические уловки, например, угрозы блокировки аккаунта, чтобы заставить людей перейти по ссылке и ввести свои данные.

По мере того как технологии шагают вперёд, методы фишинга также совершенствуются. Если раньше бдительность сводилась к проверке адреса отправителя, корректности ссылок и элементарных орфографических ошибок, то сегодня мы сталкиваемся с более изощрёнными, целенаправленными и менее заметными атаками.

Развитие фишинговых атак можно структурировать, разделив его на четыре ключевых этапа, характеризующихся определёнными временными рамками и возрастающей сложностью применяемых методов и преследуемых целей. Рассмотрим эволюцию методов фишинга в таблице 1.

Таблица 1 - Классификация эволюции фишинговых атак [1]

	Ключевые характеристики	Примеры	Методы противодействия
Примитивный массовый фишинг (1990-е – ~2005)	Широкие нецелевые рассылки, низкое качество, лёгкое обнаружение	Письма от «банка» с просьбой подтвердить данные	Базовые фильтры спама, обучение пользователей распознаванию очевидных признаков (орфографические ошибки, подозрительные адреса отправителей), проверка URL перед кликом
Технологический фишинг (~2005 – ~2015)	Использование уязвимостей, трояны, улучшенный дизайн	Внедрение кейлоггеров, фишинговые сайты-клоны	Антивирусное ПО, файерволы, регулярное обновление ПО для закрытия уязвимостей, двухфакторная аутентификация (2FA), использование безопасных браузеров с проверкой сертификатов
Целевой фишинг (~2010 – по н.в.)	Точечные атаки на конкретных людей/ компании, социальная инженерия	Целевые письма от имени коллеги или руководства	Повышенная киберграмотность, тренировки по распознаванию фишинга, строгие процедуры проверки запросов на перевод средств/данных, сегментация сетей для ограничения доступа
Высокотехнологичный фишинг (~2018 – по н.в.)	Использование AI, глубоких фейков, автоматизации	Deepfake-звонки, AIгенерация писем	Поведенческий анализ и AI-детекция аномалий, биометрическая и многофакторная аутентификация (MFA), использование кодовых слов/фраз для подтверждения критических запросов, продвинутые системы мониторинга трафика и почтовых угроз

Трансформация фишинга привела к переходу от грубых, массовых рассылок с очевидными недочётами к тонким, таргетированным атакам. Если раньше защита строилась преимущественно на технических средствах (спам-

фильтрах, антивирусах), то ныне фундаментом интернет-безопасности является осведомлённость и осторожность самого пользователя.

Для предотвращения ввода пользователями конфиденциальной информации на фишинг-сайтах используются различные технологии. В настоящее время популярные браузеры оснащены защитой от фишинга. Многие компании, специализирующиеся на разработке систем защиты от киберугроз, создают программное обеспечение, включающее в себя фильтры фишинг-сайтов [3].

В корпоративном контексте фишинг представляет собой преднамеренное киберпреступление, направленное на сотрудников. Злоумышленники используют вводящие в заблуждение коммуникации (преимущественно электронные письма) с целью получения доступа к конфиденциальным данным компании, побуждения к переходу по вредоносным URL-адресам или загрузке потенциально опасных файлов.

Согласно данным компании F6, сектор розничной торговли - основная мишень для фишинговых атак, составляя 50% всех случаев, а скам-атаки занимают 32%.

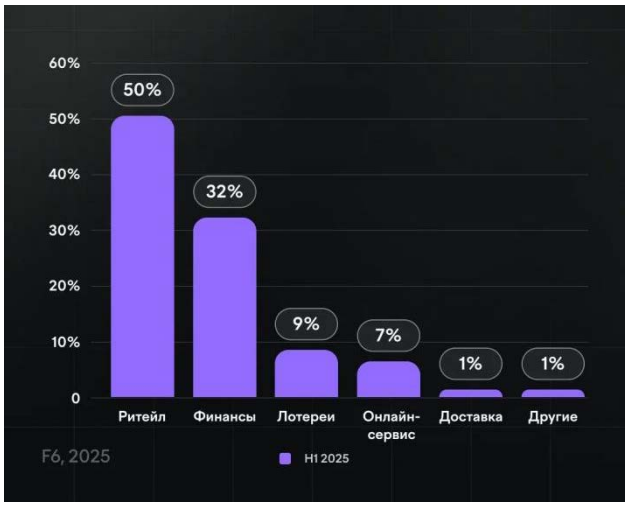

Рисунок 1 - Фишинговые атаки по отраслям (топ-5) [5]

Корпоративный фишинг представляет собой комплексную угрозу для бизнеса, проявляющуюся в нескольких ключевых аспектах. Прежде всего, это прямые финансовые убытки, вызванные мошенническими переводами,

особенно когда злоумышленники имитируют руководство для срочных платежей. Далее, фишинг чреват утечкой ценной информации, включая коммерческие секреты, интеллектуальную собственность и персональные данные. Не менее серьёзным последствием является ущерб репутации, выражающийся в потере доверия клиентов и партнёров, негативном освещении в прессе и потенциальных судебных разбирательствах. Кроме того, успешные атаки открывают злоумышленникам доступ к внутренней сети, позволяя распространять вредоносное ПО и проводить дальнейшие деструктивные действия. Особую тревогу вызывает риск атак на цепочки поставок через уязвимости стороннего ПО.

Защита сотрудников от фишинговых атак в корпоративной среде основывается на трёх главных направлениях: обучении персонала, технических средствах и организационных процедурах.

Обучение персонала является первым рубежом обороны. Регулярные тренинги, имитации фишинговых атак и практические занятия помогают сотрудникам распознавать подозрительные письма, проверять адреса отправителей, анализировать ссылки и правильно реагировать на потенциальные угрозы. Рекомендуется проводить такие занятия не реже одного раза в квартал и стимулировать сотрудников сообщать о подозрительной активности.

Технические меры включают внедрение многофакторной аутентификации (MFA) для защиты учётных записей; настройку почтовых протоколов SPF, DKIM и DMARC, которые препятствуют подделке домена; использование искусственного интеллекта для фильтрации опасных писем и ссылок; а также применение систем предотвращения утечек данных (DLP) и принципа минимальных привилегий для ограничения доступа к важным ресурсам.

Организационные меры подразумевают простую процедуру уведомления о фишинге, например, кнопку «Сообщить о фишинге» в почтовом клиенте;

разработку плана реагирования на инциденты с понятными инструкциями для сотрудников; проверку финансовых запросов и конфиденциальной информации через дополнительные каналы связи; а также использование защищённых мессенджеров для внутреннего общения.

Кроме того, важны регулярные обновления программного обеспечения, мониторинг сетевого трафика, блокировка подозрительных доменов и проведение периодических тестовых фишинговых кампаний для оценки эффективности защиты.

Главный принцип заключается в том, что ни одна мера не обеспечивает абсолютной безопасности. Только комплексный подход, объединяющий людей, технологии и процессы, способен обеспечить надёжную защиту от фишинга.

Библиографический список:

1. Гавриченко, Н. Е. Эволюция фишинга: от примитивных писем к deepfake и целевым атакам / Н. Е. Гавриченко // Интернет изнутри. – 2025. – № 23. – С. 22-25. – EDN GUAJLL.

2. Д. С. Ан, А. С. Зуфарова Классификация фишинга: различные типы и способы реализации атак // Информатика. Экономика. Управление / Informatics. Economics. Management. 2025. №1. URL: https://cyberleninka.ru/article/n/klassifikatsiya-fishinga-razlichnye-tipy-i-sposoby-realizatsii-atak.

3. Данько О. С., Медведева Т. А. ИССЛЕДОВАНИЕ ТЕХНИК ФИШИНГА И МЕТОДОВ ЗАЩИТЫ ОТ НЕГО // Молодой исследователь Дона. 2021. №3 (30). URL: https://cyberleninka.ru/article/n/issledovanie-tehnik-fishinga-i-metodov-zaschity-ot-nego.

4. Лаврищева О. А. Криминологическая характеристика преступности в сфере компьютерных технологий // Нравственные императивы в праве, образовании, науке и культуре : сб. материалов IX Международного молодежного форума (г. Белгород, 21 мая 2021 г.). – Белгород, 2021. С. 219–226.

5. F6 : официальный сайт. — URL: https://www.f6.ru/