

УДК 004.056.5

URL: <https://ptsj.bmstu.ru/catalog/icec/insec/1121.html>

МЕТОДЫ ЗАЩИТЫ ОТ ФИШИНГОВЫХ АТАК В КОРПОРАТИВНЫХ СЕТЯХ

Ю.Д. Дронов

dronovyud@student.bmstu.ru

Е.В. Глинская

glinskaya@bmstu.ru

SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Рассмотрена актуальная проблема защиты корпоративных информационных систем от фишинговых атак. Проанализированы современные виды фишинга, включая целевой фишинг (spear phishing) и атаки через служебные сообщения (Business Email Compromise). Описаны комплексные подходы к противодействию, сочетающие технические средства (системы фильтрации почтового трафика, антивирусное программное обеспечение с поведенческим анализом, двухфакторную аутентификацию) и организационные меры (регулярное обучение сотрудников, проведение учебных фишинговых кампаний). Особое внимание уделено роли искусственного интеллекта и машинного обучения в прогнозировании и предотвращении атак. На основе сравнительного анализа эффективности различных методов сделан вывод о необходимости реализации многоуровневой системы защиты, адаптированной под конкретные угрозы и человеческий фактор. В работе подчеркнуто, что только сочетание технологий и повышения киберграмотности персонала позволяет существенно снизить риски успешных фишинговых атак.

Ключевые слова: фишинг, корпоративная безопасность, двухфакторная аутентификация, киберграмотность, почтовые угрозы, человеческий фактор, машинное обучение, инциденты информационной безопасности

Введение. Фишинг (от англ. *fishing* — «рыбная ловля», «выуживание») представляет собой вид интернет-мошенничества, с помощью которого злоумышленники пытаются украсть важную информацию: логины, пароли, номера карт и другие конфиденциальные данные. Фишинг остается одним из наиболее распространенных и опасных методов кибератак на организации. По данным последних исследований, более 90 % успешных кибервторжений начинаются именно с фишинговых писем. Высокая эффективность фишинга обусловлена эксплуатацией человеческого фактора — самого уязвимого звена в системе безопасности. Злоумышленники постоянно совершенствуют тактики, переходя от массовых рассылок к целевым атакам (spear phishing) и методам социальной инженерии, что делает их письма трудно выявляемыми для традиционных систем защиты.

Цель данной работы — систематизация и анализ современных методов защиты корпоративных сетей от фишинговых атак. В задачи исследования

входят классификация видов фишинга, оценка эффективности технических и программных средств защиты, а также разработка рекомендаций по построению комплексной системы противодействия, учитывающей как технологические, так и организационные аспекты. Актуальность темы обусловлена растущим ущербом от утечек конфиденциальных данных и финансовых потерь, к которым приводят успешные фишинговые атаки.

Классификация фишинговых атак и современные тенденции. Современный фишинг можно классифицировать по нескольким ключевым признакам: цель атаки, канал доставки и степень целевого подхода [1].

Целевой фишинг (Spear Phishing) характеризуется предварительным сбором информации о жертве (должность, круг общения, проекты). Такие письма персонализированы и часто имитируют переписку с руководством или доверенными контрагентами, что значительно повышает вероятность успеха.

Фишинг через служебные сообщения (Business Email Compromise — BEC) направлен на получение финансовой выгоды путем мошеннического перевода средств. Атакующий, используя скомпрометированный или поддельный почтовый аккаунт сотрудника, отдает распоряжение бухгалтерии или финансовому отделу перевести деньги на контролируемый злоумышленниками счет.

Смифишинг (SMS-фишинг) и вишинг (голосовой фишинг) становятся все более популярными каналами атак, обходящими традиционные почтовые фильтры.

Эволюция фишинговых атак демонстрирует тенденцию к повышению изощренности и использованию методов искусственного интеллекта для генерации убедительного текста и подделки голоса. Это требует адекватного развития и систем защиты.

Технические методы защиты. Технические средства представляют собой первый рубеж обороны от фишинга.

Системы фильтрации почтового трафика. В современных почтовых шлюзах безопасности (например, на базе решений Cisco Email Security, Proofpoint, Kaspersky Secure Mail Gateway) используется комбинация методов для обнаружения угроз:

- *статический анализ URL и вложений:* проверка ссылок на репутацию в базах данных угроз, анализ файлов в песочнице (sandbox) перед доставкой пользователю;

- *машинное обучение:* модели, обученные на миллионах образцов легитимных и фишинговых писем, позволяют выявлять новые, ранее не известные угрозы по косвенным признакам (стилистика письма, метаданные, структура содержимого).

Антифишинговые решения на уровне браузера и рабочей станции. Браузеры и антивирусные продукты предупреждают пользователя о переходе на подозрительные сайты, сверяя домены с черными списками и анализируя поведение веб-страниц.

Двухфакторная аутентификация (2FA). Является критически важным элементом защиты. Даже в случае компрометации учетных данных злоумышленник не сможет получить доступ к системе без второго фактора (например, кода из мобильного приложения или SMS). Внедрение 2FA для доступа к корпоративной почте, системам документооборота и финансовым приложениям снижает успешность атак на 70...80 % [2].

Организационные методы и работа с персоналом. Поскольку технические средства не могут обеспечить 100%-ную защиту от целевого фишинга, ключевую роль в обеспечении безопасности играет подготовка пользователей [3].

Обучение и повышение осведомленности. Регулярное проведение тренингов по основам кибергигиены является обязательным элементом программы безопасности. Сотрудников необходимо обучать идентифицировать признаки фишинговых писем:

- незнакомый адрес отправителя или незначительные отклонения в доменном имени [4];
- срочность и давление в тексте письма («Срочно переведите платеж!», «Ваш аккаунт будет заблокирован в течение часа»);
- просьба предоставить конфиденциальные данные или перейти по ссылке для «подтверждения» информации.

Учебные фишинговые кампании. Наиболее эффективным методом обучения является проведение контролируемых учебных атак [5]. Специализированные платформы (например, KnowBe4, Infosecurity) позволяют отправлять сотрудникам имитационные фишинговые письма и отслеживать, кто из них «клюнул» на удочку. Это позволяет выявить наиболее уязвимые группы сотрудников и дать им целевое обучение. Практика показывает, что после регулярного проведения таких кампаний уровень успешных учебных атак падает с 30...40 до 5...10 % в течение года [6].

Четкие регламенты и процедуры. В организации должны быть установлены простые и понятные правила, регламентирующие действия сотрудников в случае получения подозрительного письма (например, «не переходить по ссылкам, не открывать вложения, сообщить в ИТ-отдел»). Также обязательны процедуры двойного подтверждения для финансовых операций, особенно при изменении реквизитов контрагентов [7].

Комплексный подход и анализ эффективности. Наиболее эффективной стратегией является построение многоуровневой (эшелонированной) защиты, которая сочетает технические и организационные меры [8].

Проведенный анализ показывает, что внедрение только почтового фильтра с ML-модулями позволяет блокировать до 95 % массового фишинга. Добавление обязательной двухфакторной аутентификации сводит на нет риск компрометации учетных записей даже при утечке паролей [9]. Однако против целевых атак (BEC, spear phishing) эти меры могут оказаться недостаточными, поскольку злоумышленник может использовать легитимные, но скомпрометированные аккаунты. Именно здесь на первый план выходят организационные меры. Регулярное обучение и учебные кампании формируют у сотрудников «иммунитет» к социальной инженерии, превращая их из самого слабого звена в активный элемент системы безопасности.

Заключение. Защита от фишинговых атак является комплексной задачей, не имеющей универсального технического решения. Современные угрозы, особенно целевой фишинг и BEC, требуют сочетания передовых технологий (машинное обучение, двухфакторная аутентификация) с непрерывной работой по повышению киберграмотности сотрудников [10].

Проведенное исследование подтверждает, что максимальную эффективность демонстрирует многоуровневая система защиты, в которой технические средства минимизируют поток угроз, а подготовленный персонал способен надежно идентифицировать и корректно реагировать на те атаки, которые обошли автоматические фильтры. Дальнейшее развитие систем защиты будет связано с более активным использованием искусственного интеллекта для поведенческого анализа и прогнозирования атак, а также с персонализацией программ обучения для разных категорий пользователей внутри организации.

Литература

- [1] Verizon. *2023 Data Breach Investigations Report*. Alexandria, VA, Verizon, 2023, 89 p.
- [2] Володин А.А., Глинская Е.В. Развитие и проблемы использования искусственного интеллекта в области информационной безопасности. *Политехнический молодежный журнал*, 2024, № 02 (91). URL: <https://ptsj.ru/catalog/icsec/insec/969.html> (дата обращения 15.10.2025).
- [3] Proofpoint. *State of the Phish Report 2024*. Sunnyvale, Proofpoint, 2024, 29 p.
- [4] Бочнев Н.А., Харисов А.Р. Надежные методы аутентификации в государственных и корпоративных информационных системах: принципы, технологии и перспективы. *Вестник науки*, 2024, № 12 (81), т. 5, ч. 1. с. 642–649.
- [5] KnowBe4. *Phishing Benchmarking Report 2023*. Clearwater, KnowBe4, 2023, 35 p.
- [6] Google. *Phishing Activity Trends Report*. Mountain View, Google, 2023.

- [7] Mansfield-Devine S. The rise of AI-powered phishing. *Computer Fraud & Security*, 2021, vol. 2021, no. 5, pp. 10–15.
[https://doi.org/10.1016/S1361-3723\(21\)00050-5](https://doi.org/10.1016/S1361-3723(21)00050-5)
- [8] Silgado A.P. et al. Leveraging User Behavior Analytics for Early Phishing Detection. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 543–556.
- [9] ENISA. *Cyber Security Culture in Organisations*. Heraklion, European Union Agency for Network and Information Security, 2018, 78 p. URL: <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations> (accessed 15.10.2025).
- [10] Petersen R., Santos D., Smith M.C., Wetzal K.A., Witte G. *Workforce Framework for Cybersecurity (NICE Framework)*. NIST Special Publication 800-181, Rev. 1. Gaithersburg, National Institute of Standards and Technology, 2020, 27 p.
<https://doi.org/10.6028/NIST.SP.800-181r1>

Поступила в редакцию 25.11.2025

Дронов Юрий Денисович — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:

Дронов Ю.Д., Глинская Е.В. Методы защиты от фишинговых атак в корпоративных сетях. *Политехнический молодежный журнал*, 2026, № 04(105). URL: <https://ptsj.bmstu.ru/catalog/icec/insec/1121.html>

METHODS OF PROTECTION AGAINST PHISHING ATTACKS IN CORPORATE NETWORKS

Yu.D. Dronov

dronovyud@student.bmstu.ru

E.V. Glinskaya

glinskaya@bmstu.ru

SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

This article examines the pressing issue of protecting corporate information systems from phishing attacks. Modern types of phishing are analyzed, including spear phishing and Business Email Compromise. Comprehensive countermeasures are described, combining technical tools (mail traffic filtering systems, antivirus software with behavioral analysis, and two-factor authentication) and organizational measures (regular employee training and training phishing campaigns). Particular attention is paid to the role of artificial intelligence and machine learning in predicting and preventing attacks. Based on a comparative analysis of the effectiveness of various methods, the need to implement a multilayered security system tailored to specific threats and the human factor is substantiated. The study emphasizes that only a combination of technologies and improved cyberliteracy among personnel can significantly reduce the risk of successful phishing attacks.

Keywords: phishing, corporate security, two-factor authentication, cyberliteracy, email threats, human factor, machine learning, information security incidents

Received 25.11.2025

Dronov Yu.D. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific Advisor — Basarab M.A., Dr. Sc. (Phys.-Math.), Head of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:

Dronov Yu.D., Glinskaya E.V. Methods of protection against phishing attacks in corporate networks. *Politekhnikheskiy molodezhnyy zhurnal*, 2026, no. 04(105). (In Russ.). URL: <https://ptsj.bmstu.ru/catalog/icec/insec/1121.html>