# ФИШИНГ И АНТИФИШИНГ. КАК ЗАЩИТИТЬ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНОЙ СРЕДЕ

*Безбородов Д.В.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Латушко М.М.*

**Аннотация.** В условиях стремительной цифровизации все сферы жизни, включая государственные и корпоративные структуры, сталкиваются с возрастающим числом киберугроз. Среди них фишинг — один из наиболее распространённых и эффективных методов социальной инженерии. В данной научной работе рассматриваются современные типы фишинга, методы его детектирования и предотвращения, особенности противодействия в корпоративной и государственной среде, а также перспективы развития антифишинговых технологий. Особое внимание уделено специфике угроз для силовых структур и методам их нейтрализации.

В условиях стремительной цифровизации все сферы жизни, включая государственные и корпоративные структуры, сталкиваются с возрастающим числом киберугроз. Среди них фишинг — один из наиболее распространённых и эффективных методов социальной инженерии. В данной научной работе рассматриваются современные типы фишинга, методы его детектирования и предотвращения, особенности противодействия в корпоративной и государственной среде, а также перспективы развития антифишинговых технологий. Особое внимание уделено специфике угроз для силовых структур и методам их нейтрализации.

Цифровая трансформация значительно повысила зависимость бизнеса, государства и общества от информационных технологий. Это сделало киберпространство приоритетной целью для злоумышленников. Одной из самых массовых и сложных к выявлению угроз остаётся фишинг. Его эффективность обусловлена тем, что он эксплуатирует человеческий фактор — доверие, недостаточную осведомлённость, усталость, повседневную рутину. В отличие от технических атак, фишинг требует минимальных ресурсов, но способен нанести колоссальный ущерб.

Для силовых структур, обладающих особым статусом и обрабатывающих чувствительную информацию, фишинговые атаки представляют особую опасность. Их успешное проведение может повлечь утечку государственной тайны, нарушение работы критически важных систем и компрометацию оперативных мероприятий.

Эволюция фишинга:

Исторически фишинг развивался от примитивных писем с орфографическими ошибками до сложных, персонализированных атак, которые используют данные из социальных сетей, корпоративных ресурсов и утечек. Сегодня злоумышленники применяют методы таргетирования, глубокого изучения поведения жертвы (behavioral profiling), а также технологии deepfake и искусственный интеллект.

Классификация фишинга и его признаки:

- Email-фишинг — массовая рассылка писем с вредоносными ссылками или вложениями;
- Spear phishing — атаки, ориентированные на конкретных лиц с персонализированным содержанием;
- Whaling — фишинг, нацеленный на руководителей и управленцев высокого уровня;
- Vishing — телефонные звонки, маскирующиеся под службы поддержки;
- Smishing — фишинг через SMS и мессенджеры;
- Фарминг — перенаправление пользователя на фальшивые сайты посредством DNS-отравления.

Основные признаки фишинга:

- Давление на пользователя: срочные просьбы, угрозы;
- Ошибки в орфографии, непривычная стилистика;
- Поддельные адреса отправителей и доменные имена;
- Запросы конфиденциальной информации.

Силовые ведомства являются приоритетной целью фишинговых кампаний из-за:

- наличия закрытой информации;
- использования устаревших каналов связи;
- ограниченного уровня цифровой грамотности у отдельных сотрудников;
- сложности многоуровневой структуры и распределённости систем управления.

Типовые сценарии атак включают:

- рассылку вредоносных писем с темами приказов и распоряжений;
- имитацию обращений от вышестоящих инстанций;
- фальсификацию писем из государственных структур.

Методы защиты и технологии антифишинга

- Аутентификация и шифрование: внедрение S/MIME, TLS, двухфакторной аутентификации;
- Проверка отправителей (SPF, DKIM, DMARC): предотвращение подделки доменов;
- SIEM-системы и поведенческий анализ: обнаружение аномалий на основе логов;
- Обновление антивирусов и прокси-фильтров: своевременная реакция на новые угрозы;
- Изоляция среды выполнения вложений (sandboxing).

Дополнительные предложения по усилению защиты:

- Внедрение автоматизированных систем обнаружения фишинга на основе нейросетей, способных адаптироваться к новым паттернам угроз;

- Использование honeypot-механизмов для анализа поведения атакующих и выявления источников фишинговых атак;

- Создание межведомственных центров быстрого реагирования на фишинговые инциденты с возможностью оперативного обмена информацией;

- Разработка специализированных решений для мобильных устройств, включая антифишинговые фильтры на уровне операционной системы;

- Внедрение киберучений с фокусом на имитацию фишинговых сценариев для формирования устойчивых поведенческих навыков у сотрудников.

Ключевым фактором устойчивости к фишингу является сознательное поведение сотрудников. Для этого необходимо:

- регулярное проведение тренингов и тестов с элементами геймификации;
- формирование каналов оперативного оповещения и отчётности о подозрительных письмах;
- развитие культуры кибербезопасности и обратной связи внутри подразделений.

По данным ENISA, в 2023 году фишинг стал причиной более 36% всех инцидентов информационной безопасности в ЕС. В России, по отчётам ФСТЭК, около 40% атак на госорганы связаны с фишинговыми письмами. Это подтверждает высокую актуальность темы.

Будущее антифишинга связано с:

- применением ИИ для анализа аномального поведения пользователей;
- интеграцией антифишинга в архитектуру Zero Trust;
- развитием поведенческой аналитики (UEBA);
- защитой от голосовых и видеофейков;
- международным обменом данными о фишинговых доменах и IP-адресах;
- внедрением интеллектуальных помощников и систем обучения.

Фишинг — это вызов, который требует междисциплинарного подхода. Только комплексные меры, сочетающие технологии, регламенты и обучение, могут гарантировать устойчивость к

фишинговым угрозам. В условиях роста гибридных угроз и активизации внешнего вмешательства, особенно для силовых структур, тема антифишинга становится вопросом не только информационной, но и национальной безопасности.

***Список использованных источников:***

1. IBM Security Data Breach Report 2024.
2. ENISA Threat Landscape 2023.
3. Verizon Data Breach Investigations Report (DBIR) 2023.
4. Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World."
5. Соловьёв А.В., "Информационная безопасность: Учебное пособие." — М.: Инфра-М, 2022.
6. Anti-Phishing Working Group Reports.
7. OWASP Phishing Awareness Guide.
8. NIST SP 800-61: Computer Security Incident Handling Guide.
9. ФСТЭК России. Методические рекомендации по обеспечению защиты информации.