АНАЛИЗ СОВРЕМЕННЫХ ФИШИНГОВЫХ АТАК И МЕТОДОВ ЗАЩИТЫ ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

А. А. Фирсов, А. С. Герасимов

Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Проанализированы современные фишинговые атаки, усилившиеся применением искусственного интеллекта и технологий глубоких подделок. Рассмотрены тенденции автоматизации и персонализации атак, показана ограниченность традиционных средств защиты. Предложен многоуровневый подход, включающий машинное обучение, поведенческий анализ и обучение персонала.

Ключевые слова: фишинг, социальная инженерия, информационная безопасность, искусственный интеллект, методы защиты.

ANALYSIS OF MODERN PHISHING ATTACKS AND METHODS OF PROTECTION AGAINST SOCIAL ENGINEERING

A. A. Firsov, A. S. Gerasimov

Belarusian state university of informatics and radioelectronics, Minsk

The paper analyzes modern phishing attacks that have intensified due to the use of artificial intelligence and deepfake technologies. Trends of automation and personalization of attacks are considered, and the limitations of traditional protection methods are demonstrated. A multi level approach is proposed, including machine learning, behavioral analysis, and personnel training.

Keywords: phishing, social engineering, information security, artificial intelligence, protection methods.

Актуальность темы обусловлена экспоненциальным ростом сложности и масштабов фишинговых атак, усиленных повсеместным использованием технологий искусственного интеллекта. По данным аналитического отчета «Лаборатории Касперского» о трендах киберугроз для бизнеса, в 2024–2025 гг. наблюдается резкий рост целевых фишинговых кампаний, использующих генеративный искусственный интеллект (далее – ИИ) для создания гиперреалистичного контента. Согласно отчету, такие атаки становятся основной причиной инцидентов информационной безопасности в корпоративной среде [1]. Угроза перестала быть исключительно цифровой, активно развиваются гибридные атаки, сочетающие электронную почту, мессенджеры и телефонные звонки.

Целью работы является анализ современных трендов в фишинговых атаках с использованием ИИ и разработка комплексной модели защиты для организаций критической информационной инфраструктуры. Для достижения цели поставлены следующие задачи: проанализировать случаи использования генеративного ИИ и deepfake-технологий в фишинге, оценить эффективность традиционных систем защиты и предложить усовершенствованный многоуровневый подход.

Ключевой тренд 2024–2025 годов – полная автоматизация и гиперперсонализация фишинговых кампаний с помощью ИИ. Атаки типа Business Email Compromise стали использовать deepfake-аудио для имитации голосов руководителей в звонках после отправки фишингового письма, что многократно повышает доверие жертвы. Как показал анализ «Лаборатории Касперского», злоумышленники активно эксплуатируют уязвимости в цепочках поставок программного обеспечения и используют сервисы-конструкторы фишинговых страниц (Phishing-as-a-Service), доступные в даркнете [1]. Это позволяет киберпреступникам с низким уровнем технической подготовки запускать масштабные и эффективные кампании. Основными векторами остаются smishing (SMS-фишинг) с использованием поддельных уведомлений от служб доставки и банков, а также фишинг в корпоративных мессенджерах.

Методы и средства защиты требуют адаптации к новым реалиям. Традиционные сигнатурные методы анализа почты показывают низкую эффективность против атак, генерируемых ИИ. На первый план выходят поведенческие анализаторы и системы на базе машинного обучения. Критически важным становится внедрение строгих регламентов проверки любых распоряжений, связанных с финансовыми операциями или передачей конфиденциальных данных. Как подчеркивается в обзоре Национального координационного центра по компьютерным инцидентам Беларуси, основой защиты является непрерывное обучение персонала с применением тренажеров, имитирующих реальные атаки с элементами глубоких подделок [2]. Пользователи должны быть обучены распознавать не только традиционные признаки фишинга, но и новые триггеры, связанные с использованием ИИ.

Проведенный анализ подтверждает, что фишинг в 2025 г. трансформировался в высокотехнологичную угрозу, борьба с которой требует применения предиктивных и поведенческих систем защиты. Успешное противодействие невозможно без интеграции трех ключевых компонентов: продвинутых технических средств (ML/AI-аналитика), строгих организационных процедур и постоянного повышения киберграмотности персонала, адаптированного к новым методам социальной инженерии. Дальнейшее развитие защитных механизмов должно быть направлено на проактивное выявление угроз, в том числе на основе рекомендаций профильных организаций [1, 2].

Литература

1 Лаборатория Касперского. Актуальные тренды киберугроз для бизнеса: 2024–2025 гг. – Kaspersky, 2025. – URL: https://www.kaspersky.ru/enterprise-security/resources/white-papers (дата обращения: 11.10.2025).

2. Национальный координационный центр по компьютерным инцидентам Республики Беларусь (НКЦКИ). Обзор основных угроз информационной безопасности в Республике Беларусь за 2024 год / ГосСОПКА. – Минск, 2025. – 78 с. – URL: https://cert.gov.by/ (дата обращения: 11.10.2025).