УДК 004.056.5

Загиров Р.А.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

Научный руководитель:
Кузьмина У.В.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

ЗАЩИТА ИНФОРМАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

Аннотация. В статье рассматриваются методы защиты информации от целевого фишинга в автоматизированных системах. Описываются основные угрозы, связанные с фишинг-атаками, и предлагаются способы предотвращения таких атак с использованием современных технологий, таких как многослойная аутентификация, анализ поведения пользователей и машинное обучение. Подчеркивается важность интеграции этих подходов в существующие системы для повышения уровня безопасности и предотвращения утечек конфиденциальных данных.

Ключевые слова: защита информации, фишинг, аутентификация, машинное обучение, безопасность.

Целевой фишинг (spear phishing) является одной из самых распространенных и разрушительных угроз в области кибербезопасности, направленных на получение конфиденциальной информации, такой как пароли, личные данные и корпоративные сведения, с помощью манипуляций и социальных инженерий. Эффективность фишинговых атак зависит от тщательной подготовки и использования специфической информации о целевой аудитории, что делает их особенно опасными в контексте автоматизированных информационных систем.

Применение технологий защиты от целевого фишинга требует всестороннего анализа угроз и инновационных методов защиты, включая использование методов машинного обучения для автоматического выявления фишинговых ссылок и социальную инженерию для обеспечения человеческого барьера защиты. Данная теоретическая часть посвящена исследованию применения методов защиты от фишинга, основанных на социальных инженерных методах и машинном обучении, с учетом существующих научных разработок [1–2].

Социальная инженерия представляет собой метод манипуляции людьми с целью получения доступа к конфиденциальной информации или изменения поведения с использованием психологических факторов. В контексте фишинговых атак, социальная инженерия играет ключевую роль

в повышении эффективности атак, направленных на специфические цели. Одно из исследований подчеркивает, что фишинг как таргетированная атака использует не только технические уязвимости, но и слабости человеческой психологии. Основным механизмом является создание ложного чувства доверия у жертвы, что приводит ее к необдуманным действиям, таким как переход по вредоносной ссылке или предоставление личной информации [1].

Таргетированные атаки часто включают персонализированные сообщения, которые используют данные из социальных сетей или корпоративных систем для создания более убедительных фишинговых писем. Жертва получает сообщение, которое кажется исходящим от коллеги или руководителя, что значительно повышает вероятность того, что она откроет вредоносное вложение или кликнет по фальшивой ссылке. Данный подход требует от злоумышленников не только технической подготовки, но и знания психологии, что делает его еще более опасным.

Важным аспектом в контексте социальной инженерии является использование фальшивых сайтов, которые копируют интерфейсы известных интернет-ресурсов, что затрудняет обнаружение фишинга. По сути, это искусственная манипуляция восприятием, в ходе которой жертва не воспринимает сообщение как угрозу, доверяя отправителю [2].

Одной из современных тактик в реализации фишинговых атак является использование документов, созданных в приложениях Microsoft Office, как контейнеров для вредоносных программ (пейлоадов). В одном из исследований рассматривается использование уязвимостей в офисных приложениях для внедрения и распространения вредоносного кода. Документы, содержащие макросы или скрытые объекты, могут быть отправлены жертве как нормальные рабочие файлы, что делает этот способ чрезвычайно эффективным.

Когда пользователь открывает такой документ, он может активировать скрытый код, который, в свою очередь, запускает пейлоад – вредоносную программу, которая может записывать нажатия клавиш, красть данные или выполнять другие действия в фоновом режиме. В отличие от традиционных методов фишинга, где жертва должна перейти по ссылке, здесь достаточно просто открыть файл, чтобы подвергнуться атаке. Это делает использование документов MS Office весьма эффективным методом для распространения фишинга, так как многие пользователи привыкли работать с такими файлами и не воспринимают их как потенциально опасные [2].

Применение данной техники требует от злоумышленников не только технических навыков, но и знания специфики работы с офисными документами, что позволяет им скрывать вредоносные элементы в таких форматах, как Word или Excel. Обычные антивирусные программы могут не всегда эффективно выявлять такие угрозы, что увеличивает риск успешной атаки.

Современные технологии машинного обучения (МЛ) играют важную роль в предотвращении фишинговых атак. Использование алгоритмов, способных выявлять аномалии в поведении пользователя и анализировать фишинговые ссылки, становится важной частью защиты автоматизированных систем. В одном из исследований описывается методы машинного обучения для автоматического определения фишинговых ссылок.

Машинное обучение позволяет анализировать огромные объемы данных и выявлять паттерны, которые могут указывать на фишинг. Например, алгоритмы могут анализировать ссылки, проверяя их на предмет известных признаков фишинга, таких как странные доменные имена, нестандартные символы и другие аномалии. Использование машинного обучения для анализа URL-адресов позволяет значительно повысить точность и скорость обнаружения угроз. В дополнение к этому, методы анализа текста позволяют выявить фишинговые письма, которые на первый взгляд могут выглядеть как легитимные, но при детальном анализе содержат скрытые признаки мошенничества [3].

Кроме того, подходы машинного обучения могут быть использованы для анализа поведения пользователей в системах, что позволяет детектировать подозрительные действия. Например, если пользователь начинает действовать нехарактерно для своей роли или перемещается по ресурсам, которые обычно не посещает, система может предупредить о возможной атаке или даже заблокировать доступ до выяснения причин.

Алгоритмы машинного обучения, такие как нейронные сети и методы классификации, могут использовать исторические данные для обучения и повышения точности распознавания фишинговых атак. Это позволяет системе адаптироваться и становиться более эффективной с каждым новым опытом.

Целевой фишинг остается одной из самых опасных форм киберугроз, оказывающих серьезное влияние на безопасность информации в автоматизированных системах. Эффективная защита от фишинга требует комплексного подхода, который включает как технические меры (например, использование многослойной аутентификации, фильтрация фишинговых писем, внедрение технологий машинного обучения), так и внимание к социальной инженерии, которая является основой большинства атак. Современные исследования в этой области подчеркивают необходимость создания гибких и эффективных систем защиты, которые могут быстро адаптироваться к новым угрозам. Использование инновационных технологий, таких как машинное обучение для автоматического обнаружения фишинговых ссылок, является важным шагом на пути к более безопасной цифровой среде.

Список использованных источников:

1. Казаковцев М.С., Михайлова У.В. Афанасьева М.В. Социальная инженерия в таргетированных атаках // Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 84–87.
2. Михайлова У.В., Кремлев Е.С. Использование документов MS OFFICE в качестве контейнеров пейлоада // Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 414–415.
3. Алексеев А.К., Будылин Е.С. Определение фишинговых ссылок с использованием методов машинного обучения / Оригинальные исследования (ОРИС). 2024 № 7 (14). С. 116–120.

Zagirov R.A.
Nosov Magnitogorsk State Technical University, Magnitogorsk

Scientific supervisor:
Kuzmina U.V.
Nosov Magnitogorsk State Technical University, Magnitogorsk

INFORMATION PROTECTION AGAINST SPEAR PHISHING IN AUTOMATED SYSTEMS

Abstract. The article discusses methods for protecting information from targeted phishing in automated systems. It describes the main threats associated with phishing attacks and suggests ways to prevent such attacks using modern technologies, such as multi-layer authentication, user behavior analysis, and machine learning. It emphasizes the importance of integrating these approaches into existing systems to improve security and prevent leaks of confidential data.

Keywords: information security, phishing, authentication, machine learning, security.