БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 3 (114). – 9–20

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.53 DOI: 10.17212/2782-2230-2024-3-9-20

РАСПОЗНАВАНИЕ ФИШИНГОВЫХ ССЫЛОК С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ*

К.А. ЛУКМАНОВА[1], В.М. КАРТАК[2]

[1] *450076, РФ, г. Уфа, ул. Заки Валиди, 32, Уфимский университет науки и технологий, аспирант кафедры вычислительной техники и защиты информации. E-mail: lukmanova.ka@gmail.ru*
[2] *450076, РФ, г. Уфа, ул. Заки Валиди, 32, Уфимский университет науки и технологий, доктор физико-математических наук, профессор, заведующий кафедрой вычислительной техники и защиты информации. E-mail: kartak.vm@ugatu.su*

В последние годы фишинг стал одной из наиболее распространенных и опасных киберугроз. Эти атаки направлены на получение конфиденциальной информации пользователей, такой как пароли и данные банковских карт, посредством обманных сообщений или веб-сайтов, что делает проблему защиты от них актуальной как никогда. Традиционные методы защиты от фишинга, такие как черные списки и эвристический анализ, уже не справляются с темпами эволюции фишинговых атак. В связи с этим возникает необходимость в разработке более современных и интеллектуальных методов, среди которых особое место занимают методы машинного обучения. В настоящей статье рассматриваются различные методы машинного обучения, применяемые для автоматического выявления фишинговых URL. В работе представлены основные подходы, архитектуры моделей, преимущества и недостатки каждого метода, а также проведен сравнительный анализ их эффективности на реальных данных.

Ключевые слова: фишинг, машинное обучение, фишинговые URL, киберугрозы, глубокое обучение, сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), логистическая регрессия, градиентный бустинг, случайный лес, классификация, кибербезопасность, анализ сетевого трафика, анализ веб-страниц, вычислительная сложность

* Статья получена 12 августа 2024 г.

ВВЕДЕНИЕ

Фишинг – это вид кибератаки, при которой злоумышленник пытается получить конфиденциальную информацию пользователей, такую как пароли, данные банковских карт или другая личная информация, выдавая себя за доверенное лицо или организацию. Чаще всего это происходит через электронные письма или сообщения, которые содержат ссылки на поддельные веб-сайты, визуально напоминающие настоящие. Эти фальшивые сайты обычно очень похожи на легитимные, что делает их трудноразличимыми для большинства пользователей [1].

Значительное увеличение числа фишинговых атак за последние годы связано с ростом интернет-коммерции и активным использованием цифровых сервисов. Согласно отчетам по информационной безопасности фишинг является одной из наиболее распространенных форм кибератак и продолжает совершенствоваться, адаптируясь к современным защитным мерам [2]. В результате традиционные методы защиты, такие как фильтрация по черным спискам, эвристические анализаторы, сигнатуры и ручной контроль, теряют свою эффективность [3].

Одним из решений этой проблемы является применение методов машинного обучения, которые способны автоматически распознавать и классифицировать фишинговые URL на основе анализа их характеристик. Такие методы могут не только повысить точность и скорость обнаружения фишинговых ссылок, но и обеспечить устойчивость к новым, ранее неизвестным атакам.

1. КЛАССИФИКАЦИЯ МЕТОДОВ РАСПОЗНАВАНИЯ ФИШИНГОВЫХ ССЫЛОК

Для эффективного распознавания фишинговых ссылок используются различные методы машинного обучения. Все они условно делятся на несколько категорий: методы анализа содержимого URL, методы анализа содержимого веб-страницы, методы анализа сетевого трафика и гибридные методы [4].

1.1. МЕТОДЫ НА ОСНОВЕ АНАЛИЗА СОДЕРЖИМОГО URL

Эти методы направлены на анализ характеристик URL, не углубляясь в содержимое веб-страницы. Они используют следующие признаки.

- Длина URL. Фишинговые ссылки часто имеют либо чрезмерно длинные, либо короткие URL.

- Использование поддоменов. Часто фишинговые сайты используют множество поддоменов для маскировки.
- Наличие подозрительных слов. В URL могут содержаться такие слова, как login, secure, verify, что может служить индикатором фишинга.
- Специальные символы. Например, наличие в URL символов “-”, “@”, “%”, которые часто используются для обмана пользователей.

Эти признаки могут быть использованы в качестве входных данных для различных моделей машинного обучения, таких как логистическая регрессия, деревья решений или случайный лес. Эти модели обучаются на данных, содержащих как легитимные, так и фишинговые URL, что позволяет им выявлять закономерности и строить классификаторы, способные разделять URL на безопасные и подозрительные.

Пример исследования. В одном из исследований была использована модель логистической регрессии, обученная на наборе данных, включающем 30 000 URL. В качестве признаков использовались длина URL, количество поддоменов, наличие подозрительных слов и другие характеристики. Результаты показали, что такая модель способна с высокой точностью (около 90 %) распознавать фишинговые URL [5].

Однако основной недостаток такого подхода заключается в его ограниченности – он может не справляться с новыми видами фишинга, которые используют новые, ранее не встречавшиеся техники маскировки.

1.2. МЕТОДЫ НА ОСНОВЕ АНАЛИЗА СОДЕРЖИМОГО ВЕБ-СТРАНИЦЫ

В отличие от методов, основанных на анализе URL, этот подход требует более глубокого анализа содержимого веб-страницы. Он включает следующие аспекты.

- SSL-сертификат. Проверка наличия и подлинности SSL-сертификата, который является признаком защищенности веб-сайта.
- Соответствие доменного имени содержимому страницы. Например, если доменное имя не соответствует тематике или содержимому сайта, это может быть признаком фишинга.
- Количество и типы внешних ссылок. Фишинговые сайты часто содержат множество внешних ссылок на подозрительные ресурсы.
- Анализ текста страницы. Автоматический анализ текста на наличие ошибок, мошеннических предложений и т. д.

Эти методы требуют значительно большего количества вычислительных ресурсов по сравнению с анализом URL. Однако они позволяют выявить фишинг с высокой точностью за счет анализа контекста страницы [6, 7].

Пример исследования. В исследовании, проведенном группой ученых, использовались случайные леса и градиентный бустинг для классификации фишинговых сайтов. Такие модели обучались на большом наборе данных, содержащем как фишинговые, так и легитимные сайты. В качестве признаков использовались различные характеристики страниц, такие как наличие SSL-сертификата, метаданные и внешний вид сайта. Результаты показали, что эти методы позволяют достичь точности до 95 %, что делает их весьма эффективными для обнаружения фишинговых сайтов. Однако такой подход требует значительных вычислительных ресурсов и времени на анализ каждой страницы, и это может ограничивать его применение в реальном времени.

1.3. МЕТОДЫ НА ОСНОВЕ АНАЛИЗА ТРАФИКА

Методы анализа трафика предполагают изучение поведения пользователя и характеристик взаимодействий с веб-сайтами. Они учитывают следующие аспекты.

- Частота посещений домена. Анализируется, как часто и кем посещается данный домен.
- Время нахождения на сайте. Временны́е характеристики сессий могут свидетельствовать о ненадежности сайта.
- Повторные переходы. Повторные переходы по подозрительным ссылкам могут служить признаком фишинга.

На основе этих данных строятся поведенческие модели, которые могут выявлять аномалии, характерные для фишинговых атак. Применение методов кластеризации, таких как K-средние, позволяет группировать схожие по поведению URL и выявлять потенциально опасные.

Пример исследования. Одно из исследований изучало использование методов кластеризации для обнаружения фишинговых сайтов на основе анализа сетевого трафика. Исследователи использовали метод K-средних для классификации URL, основываясь на таких признаках, как частота посещений и время, проведенное на сайте. Результаты показали, что с помощью такого метода можно с точностью до 85 % различать фишинговые и легитимные сайты. Однако его основным недостатком является зависимость от наличия достаточного объема данных о поведении пользователей, что может ограничивать его применение на новых или редко посещаемых сайтах [8].

1.4. ГИБРИДНЫЕ МЕТОДЫ

Гибридные методы представляют собой комбинацию нескольких подходов с целью повышения точности и надежности распознавания фишинговых

ссылок. Например, можно объединить анализ URL и контент-ориентированный подход для получения более детальной информации о ссылке и странице. Это позволяет учитывать как поверхностные, так и более глубокие признаки [9].

Сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN) позволяют автоматически извлекать сложные признаки и комбинировать их для классификации. CNN хорошо подходят для анализа текстовых данных, таких как URL и текст страницы, тогда как RNN могут учитывать временны́е зависимости и историю взаимодействия с сайтом.

Пример исследования. В исследовании была предложена гибридная модель, основанная на комбинации сверточной нейронной сети для анализа URL и рекуррентной нейронной сети для анализа содержимого веб-страницы и поведения пользователя. Эта модель была обучена на большом наборе данных и показала точность распознавания фишинговых сайтов свыше 97 %. Это значительно превышает точность традиционных методов, однако требует значительных вычислительных ресурсов. Основным преимуществом такой модели является ее способность адаптироваться к новым видам фишинга и быстро обучаться на новых данных.

2. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Для оценки эффективности различных методов машинного обучения был проведен эксперимент на большом наборе данных, включающем как фишинговые, так и легитимные URL. В созданном нами наборе данных, который был загружен в систему, общее количество примеров сайтов с легитимными ссылками 1094, а количество примеров, относящихся к фишинговым URL, – 1362. Все признаки нормализованы и имеют бинарные значения для определения: от –1 до 1, где –1 означает фишинговую ссылку, 0 означает подозрительную ссылку, и 1 означает легитимную ссылку. Нулевой признак подозрительной ссылки показывает, что веб-страница может быть или фишинговой, или настоящей, т. е. ссылка содержит в себе как некоторые «законные», так и фальшивые признаки.

При помощи функции языка Python TF-IDF разделили набор данных на тестовую и обучающую выборку. Для этого использовали соотношение 20 % и 80 %. В полученной обучающей выборке содержится 1081 фишинговая запись и 883 «законные». Остальная часть отправлена в тестовую выборку.

Были протестированы следующие модели: логистическая регрессия, случайный лес, градиентный бустинг, сверточная нейронная сеть и рекуррентная нейронная сеть. Основными метриками для оценки качества моделей были

выбраны точность (accuracy), полнота (recall), F-мера (F1-score) и площадь под кривой ROC (ROC-AUC).

2.1. ЛОГИЧЕСКАЯ РЕГРЕССИЯ

Логистическая регрессия – один из простейших методов классификации, который показал себя достаточно эффективным в задачах, связанных с бинарной классификацией, таких как распознавание фишинговых URL. В проведенном эксперименте логистическая регрессия продемонстрировала средний уровень точности на уровне 88 %. Это связано с тем, что данный метод ограничен линейностью используемой модели, что не позволяет учитывать более сложные и нелинейные зависимости между признаками.

2.2. СЛУЧАЙНЫЙ ЛЕС

Случайный лес (Random Forest) – это ансамблевый метод, который использует множество деревьев решений для улучшения устойчивости и точности классификации. В эксперименте случайный лес показал более высокие результаты по сравнению с логистической регрессией, достигая точности около 92 %. Этот метод особенно хорошо справляется с задачами, в которых необходимо учитывать взаимодействие между большим числом признаков. Однако его основным недостатком является увеличение сложности модели и соответственно времени на ее обучение и предсказание.

2.3. ГРАДИЕНТНЫЙ БУСТИНГ

Градиентный бустинг – еще один ансамблевый метод, который использует последовательное построение деревьев решений с целью минимизации ошибок предыдущих моделей. В эксперименте этот метод показал одну из наилучших точностей среди классических методов машинного обучения, достигая 94 %. Градиентный бустинг особенно эффективен при наличии большого объема данных и большого числа признаков. Однако, подобно случайному лесу, он требует значительных вычислительных ресурсов, особенно при обработке больших наборов данных.

2.4. СВЕРТОЧНАЯ НЕЙРОННАЯ СЕТЬ

Сверточные нейронные сети (CNN) изначально разработаны для обработки данных с локальными зависимостями, таких как изображения, однако

они также оказались эффективными и для текстовых данных, таких как URL. В эксперименте CNN продемонстрировала высокую точность, превышающую 95 %. Это связано с ее способностью извлекать сложные признаки, которые могут быть неочевидны для классических методов машинного обучения. CNN особенно полезны для распознавания паттернов в тексте URL, что делает их мощным инструментом в задачах классификации фишинговых ссылок.

2.5. РЕКУРРЕНТНАЯ НЕЙРОННАЯ СЕТЬ

Рекуррентные нейронные сети (RNN) и их более современные версии, такие как LSTM (Long Short-Term Memory), используются для анализа последовательных данных и временны́х рядов. В контексте фишинговых ссылок они могут анализировать последовательности символов в URL или даже последовательности действий пользователя на сайте. В эксперименте RNN показала точность около 93 %, уступая CNN, но превосходя традиционные методы машинного обучения. Основное преимущество RNN заключается в ее способности учитывать контекст и историю взаимодействий, что может быть полезно для обнаружения более сложных фишинговых атак.

3. СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ

Точность и надежность. Анализ показал, что современные методы, основанные на глубоком обучении (CNN и RNN), демонстрируют наивысшую точность и надежность при распознавании фишинговых URL. Эти методы способны автоматически извлекать сложные признаки и учитывать нелинейные зависимости, что делает их более эффективными в условиях динамически меняющихся атак. Однако их использование связано с высокими вычислительными затратами, что может ограничивать их применение в условиях реального времени или на устройствах с ограниченными ресурсами.

Классические методы машинного обучения, такие как логистическая регрессия и деревья решений, показали более низкую точность, однако они имеют преимущество в скорости работы и простоте реализации. Эти методы могут быть применимы в ситуациях, когда необходимо быстрое и простое решение, не требующее значительных вычислительных ресурсов [10].

Гибкость и адаптивность. Гибридные методы, такие как комбинация CNN и RNN, показали наилучшие результаты с точки зрения адаптивности к новым атакам. Такие модели могут быть быстро переобучены на новых данных, что позволяет им эффективно справляться с новыми видами фишинго-

вых атак. Это особенно важно в условиях, когда злоумышленники постоянно адаптируют свои методы для обхода традиционных защитных мер.

Классические методы, такие как градиентный бустинг и случайный лес, также обладают определенной гибкостью, однако они требуют более частого обновления моделей и не всегда могут эффективно обрабатывать новые виды атак без значительных изменений в архитектуре модели [11].

Вычислительная сложность. Одним из ключевых факторов при выборе метода является вычислительная сложность. Методы глубокого обучения, такие как CNN и RNN, требуют значительных ресурсов для обучения и предсказания, что может ограничивать их применение в условиях реального времени. С другой стороны, классические методы, такие как логистическая регрессия и случайный лес, являются менее ресурсоемкими и могут быть использованы для быстрых предсказаний на больших объемах данных.

ЗАКЛЮЧЕНИЕ

В настоящей статье были рассмотрены различные методы машинного обучения, используемые для распознавания фишинговых URL. Мы провели сравнительный анализ нескольких моделей, включая как классические методы машинного обучения, так и современные подходы на основе глубокого обучения. Результаты показали, что гибридные методы, такие как комбинация CNN и RNN, обладают наивысшей точностью и адаптивностью. Это делает их наиболее перспективными для использования в условиях постоянно меняющейся среды киберугроз.

Однако использование глубоких нейронных сетей связано с высокими вычислительными затратами, что может ограничивать их применение в реальных условиях. В то же время более простые модели, такие как логистическая регрессия и деревья решений, обеспечивают приемлемый уровень точности при низких затратах на вычисления, что делает их подходящими для быстрого фильтрационного анализа.

В будущем целесообразно развивать методы, направленные на уменьшение вычислительной сложности моделей глубокого обучения, а также на интеграцию различных подходов для повышения общей эффективности распознавания фишинговых атак. Кроме того, важным направлением дальнейших исследований является разработка методов, способных эффективно адаптироваться к новым и неизвестным типам атак, что позволит значительно повысить уровень информационной безопасности в сети.

СПИСОК ЛИТЕРАТУРЫ

1. *Карпова Н.Е., Восканян И.И.* Угроза социальной инженерии и фишинга в современной информационной безопасности // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 69–78. – DOI: 10.17212/2782-2230-2024-2-69-78.

2. Phishing Attack Trends Report – 4Q 2023 / APWG. Phishing Activity Trends Reports. – URL: https://apwg.org/trendsreports/ (accessed 28.08.2024).

3. *Hussein S.K., Wahaballah A., Alosaimi A.* Detecting phishing websites using natural language processing // International Journal of Computer Engineering in Research Trends. – 2021. – Vol. 8 (12). – P. 220–227.

4. *Кутлыев Д.З., Шманина А.В.* Использование алгоритмов машинного обучения для защиты от URL-фишинга // Мавлютовские чтения: XV Всероссийская молодежная научная конференция. – Уфа, 2021. – Т. 4. – С. 430–435.

5. Classifying phishing URLs using recurrent neural networks / A.C. Bahnsen, I.D. Torroledo, J. Camacho, S. Villegas // 2017 APWG Symposium on Electronic Crime Research (eCrime). – IEEE, 2017. – DOI: 10.1109/ECRIME.2017.7945048.

6. Machine learning based phishing detection from URLs / O.K. Sahingoz, E. Buber, O. Demir, B. Diri // Expert Systems with Applications. – 2019. – Vol. 117. – P. 345–357.

7. *Лукманова К.А., Картак В.М.* Векторное представление слов в задаче анализа текстовых сообщений // Мавлютовские чтения: XIV Всероссийская молодежная научная конференция. – Уфа, 2020. – Т. 5, ч. 2. – Ст. 25.

8. *Артюшкина Е.С., Андирякова О.О., Тюрина Д.А.* Использование методов машинного обучения при анализе сетевого трафика и вредоносного программного обеспечения // Индустриальная экономика. – 2023. – № 4. – С. 12–15. – DOI: 10.47576/2949-1886_2023_4_12.

9. *Мухамадиева К.Б., Муминов Б.Б.* Обзор методов обнаружения фишинговых атак на основе искусственного интеллекта // Вестник Донецкого национального университета. Серия Г: Технические науки. – 2021. – № 4. – С. 37–45.

10. Beyond blacklists: learning to detect malicious web sites from suspicious URLs / J. Ma, L.K. Saul, S. Savage, G.M. Voelker // KDD '09: Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – ACM, 2009. – P. 1245–1254. – DOI: 10.1145/1557019.1557153.

11. *Dutta A.K.* Detecting phishing websites using machine learning technique // PLoS ONE. – 2021. – Vol. 16 (10). – P. e0258361. – DOI: 10.1371/journal.pone.0258361.

Лукманова Карина Александровна, аспирант кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий. Основное направление научных исследований – информационная безопасность, машинное обучение. E-mail: lukmanova.ka@gmail.ru

Картак Вадим Михайлович, доктор физико-математических наук, заведующий кафедрой вычислительной техники и защиты информации Уфимского университета науки и технологий. Область научных интересов – информационная безопасность, дискретная оптимизация. E-mail: kartak.vm@ugatu.su

DOI: 10.17212/2782-2230-2024-3-9-20

Recognition of phishing links using machine learning methods*

K.A. Lukmanova[1], V.M. Kartak[2]

[1] *Ufa University of Science and Technology, 32 Zaki Validi Street, Ufa, 450076, Russian Federation, postgraduate student at the Department of Computer Engineering and Information Security. E-mail: lukmanova.ka@gmail.ru*

[2] *Ufa University of Science and Technology, 32 Zaki Validi Street, Ufa, 450076, Russian Federation, Doctor of Physical and Mathematical Sciences, Professor, head of the Computer Engineering and Information Security Department. E-mail: kartak.vm@ugatu.su*

In recent years, phishing has become one of the most widespread and dangerous cyber threats. These attacks aim to obtain users' confidential information, such as passwords and credit card details, through deceptive messages or websites, making the issue of protection against them more relevant than ever. Traditional methods of phishing protection, such as blacklists and heuristic analysis, can no longer keep up with the evolving pace of phishing attacks. Therefore, there is a need to develop more advanced and intelligent methods, among which machine learning (ML) techniques play a significant role. This article discusses various ML methods used for automatic detection of phishing URLs. The study presents the main approaches, model architectures, advantages and disadvantages of each method, and provides a comparative analysis of their effectiveness on real data.

Keywords: phishing, machine learning, phishing URLs, cyber threats, deep learning, convolutional neural networks (CNN), recurrent neural networks (RNN), logistic regression, gradient boosting, random forest, classification, cybersecurity, network traffic analysis, web page analysis, computational complexity

* *Received 12 August 2024.*

REFERENCES

1. Karpova N.E., Voskanyan I.I. Ugroza sotsial'noĭ inzhenerii i fishinga v sovremennoĭ informatsionnoĭ bezopasnosti [Threat of social engineering and phishing in modern information security]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 69–78. DOI: 10.17212/2782-2230-2024-2-69-78.

2. APWG. *Phishing Attack Trends Report – 4Q 2023*. Available at: https://apwg.org/trendsreports/ (accessed 28.08.2024).

3. Hussein S.K., Wahaballah A., Alosaimi A. Detecting phishing websites using natural language processing. *International Journal of Computer Engineering in Research Trends*, 2021, vol. 8 (12), pp. 220–227.

4. Kutlyev D.Z., Shmanina A.V. [Using machine learning algorithms to protect against URL phishing]. *Mavlyutovskie chteniya: XV Vserossiiskaya molodezhnaya nauchnaya konferentsiya* [Mavlyutov Readings. Proceedings of the XV All-Russian Youth Scientific Conference]. Ufa, 2021, vol. 4, pp. 430–435. (In Russian).

5. Bahnsen A.C., Torroledo I.D., Camacho J., Villegas S. Classifying phishing URLs using recurrent neural networks. *2017 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2017. DOI: 10.1109/ECRIME.2017.7945048.

6. Sahingoz O.K., Buber E., Demir O., Diri B. Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 2019, vol. 117, pp. 345–357.

7. Lukmanova K.A., Kartak V.M. [Vector representation of words in the task of text message analysis]. *Mavlyutovskie chteniya: XIV Vserossiiskaya molodezhnaya nauchnaya konferentsiya* [Mavlyutov Readings. Proceedings of the XIV All-Russian Youth Scientific Conference]. Ufa, 2020, vol. 5, pt. 2, art. 25. (In Russian).

8. Artyushkina E.S., Andiryakova O.O., Tyurina D.A. Ispol'zovanie metodov mashinnogo obucheniya pri analize setevogo trafika i vredonosnogo programmnogo obespecheniya [Using machine learning methods in analyzing network traffic and malicious software]. *Industrial'naya ekonomika = Industrial Economics*, 2023, no. 4, pp. 12–15. DOI: 10.47576/2949-1886_2023_4_12.

9. Mukhamadieva K.B., Muminov B.B. Obzor metodov obnaruzheniya fishingovykh atak na osnove iskusstvennogo intellekta [Review of phishing attack detection methods based on artificial intelligence]. *Vestnik Donetskogo natsional'nogo universiteta. Seriya G: Tekhnicheskie nauki = Bulletin of Donetsk National University. Series G: Technical Sciences*, 2021, no. 4, pp. 37–45.

10. Ma J., Saul L.K., Savage S., Voelker G.M. Beyond blacklists: learning to detect malicious web sites from suspicious URLs. *KDD '09: Proceedings of the*

15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2009, pp. 1245–1254. DOI: 10.1145/1557019.1557153.

11. Dutta A.K. Detecting phishing websites using machine learning technique. *PLoS ONE*, 2021, vol. 16 (10), p. e0258361. DOI: 10.1371/journal.pone.0258361.

Для цитирования:

Лукманова К.А., Картак В.М. Распознавание фишинговых ссылок с использованием методов машинного обучения // Безопасность цифровых технологий. – 2024. – № 3 (114). – С. 9–20. – DOI: 10.17212/2782-2230-2024-3-9-20.

For citation:

Lukmanova K.A., Kartak V.M. Raspoznavanie fishingovykh ssylok s ispol'zovaniem metodov mashinnogo obucheniya [Recognition of phishing links using machine learning methods]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 3 (114), pp. 9–20. DOI: 10.17212/2782-2230-2024-3-9-20.