Построение алгоритмов машинного обучения для детектирования сайтов-мошенников

Лукьянов Дмитрий А. , Лапина Мария А. , Лапин Виталий Г. , Кучеров Николай Н.

Северо-Кавказского федерального университета, Пушкина 1, 355000, Ставрополь

Аннотация

В настоящее время с развитием информационных технологий цифровые преступления стали серьёзной угрозой для конфиденциальной информации и данных пользователей. Искусственный интеллект способен анализировать параметры сайтов и определять наличие угроз для информации. В ходе выполнения исследования были разработаны методы машинного обучения по обнаружения фишинговых сайтов, построены схемы, которые позволяют моделям машинного обучения правильно преобразовывать данные для подачи их в модели. В результате работы разработаны методы поиска фишинговых атак с использованием моделей машинного обучения, которые были протестированы на имеющихся данных, на основе полученных результатов построены графики изменения точности обнаружения нелегитимных сайтов от изменения настроек моделей.

Ключевые слова:

машинное обучения, фишинг, сайт-мошенник, KNIME, киберпреступность, кибер-атаки, поиск уязвимостей, искусственный интеллект.

1. Введение

Фишинг – тип интернет-мошенничества, целью которого является получение персональных данных пользователя: пароли, данные кредитных карт, банковские счета, почты, паспортные данные и другая конфиденциальная информация [1]. Фишинговыми атаками могут являться: поддельные письма на электронную почту от банков, провайдеров с просьбой обновить персональные данные.Термин “Фишинг” впервые прозвучал 2 января 1996 года. Упоминание о данном явлении впервые появилось в группе новостей “Usenet” под названием “AOHello” [2]. В январе 1996 года была проведена первая в истории фишинговая атака.

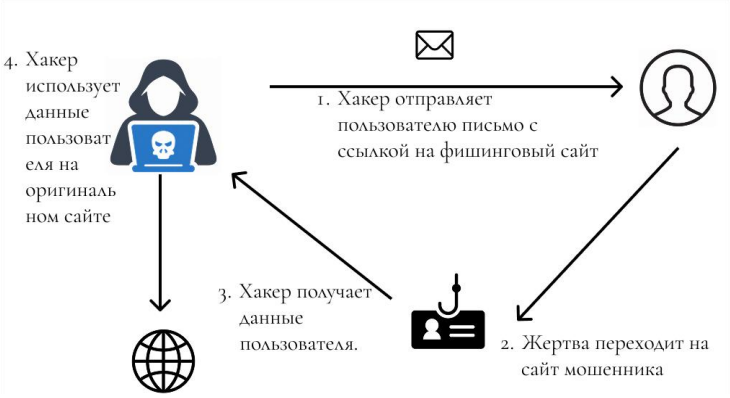

Рисунок 1 – План фишинговой атаки.

7th International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE 2025), July 7–11, 2025, Irkutsk, Russia
EMAIL: ilia.alekseev.kenig@gmail.com (A. 1); mlapina@ncfu.ru (A. 2); vitlx@yandex.ru (A. 3) ; nik.bekesh@gmail.com (A. 4)
ORCID: 0009-0009-7203-0309 (A. 1); 0000-0001-8117-9142 (A. 2); 0000-0002-0611-7002 (A. 3); 0000-0003-0337-0093 (A. 4)

ICCS-DE 2025 Workshop Proceedings
DOI: 10.47350/ICCS-DE.2025.31

В настоящее время из-за развития компьютерных технологий и широкого распространения интернета защита от фишинговых атак стала надёжнее, но хакеры придумывают новые методы атак. Выделяют следующие типы фишинговых атак: целевой фишинг [3], vishing [4], клон-фишинг [5], фишинг в поисковых системах [6].

Существующие методы защиты (фильтрация URL [7], двухфакторная аутентификация [8], обучение пользователей [9], браузерные расширения [10]) не обеспечивают полной безопасности. В связи с этим актуальной задачей становится разработка автоматизированных систем на основе машинного обучения (МО), способных анализировать параметры сайтов и выявлять фишинговые угрозы.

2. Машинное обучение

Машинное обучение (МО) – это область искусственного интеллекта, которая позволяет ему находить закономерности в данных и делать прогнозы. Программа анализирует данные, находит в них последовательности и закономерности, обучается и применяет результаты на практике, прогнозируя данные.

Для работы с машинным обучением необходим набор данных (датасет) [11], в котором внесены основные характеристики сайтов и результат. Данный датасет создан для обнаружения фишинговых сайтов, которые маскируются под легитимными ресурсами, чтобы украсть данные пользователей.

Для работы с выбранным датасетом необходимо выбрать аналитическую платформу, которая предоставляет возможность работать с машинным обучением. В данном исследование для работы была выбрана аналитическая платформа с открытым кодом – KNIME [12].

3. Модели машинного обучения

Для работы с моделями необходимо построить схему, позволяющую анализировать данные. Обобщающая модель данных моделей показана на рисунке 2.

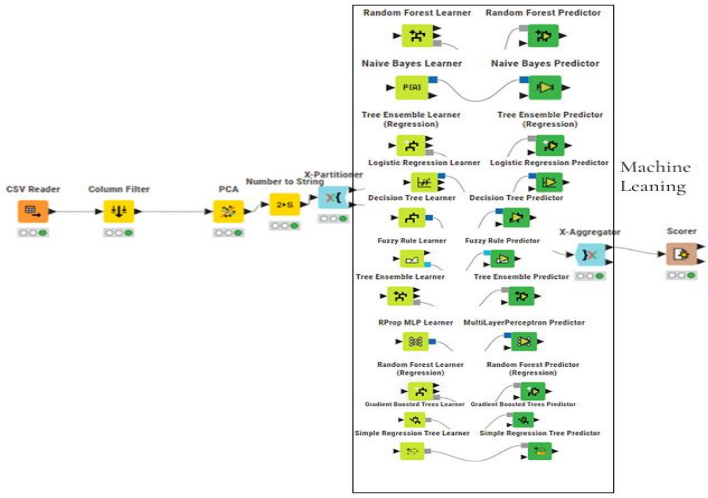

Рисунок 2 – Модели машинного обучения.

Наилучшие результаты показали ансамблевые методы:

1. Random Forest [13] — точность 96,6% (глубина дерева 20).
2. Gradient Boosted Trees [14] — точность 97,34% (глубина дерева 10).
3. Tree Ensemble [15] — точность 96,59% (глубина дерева 20).

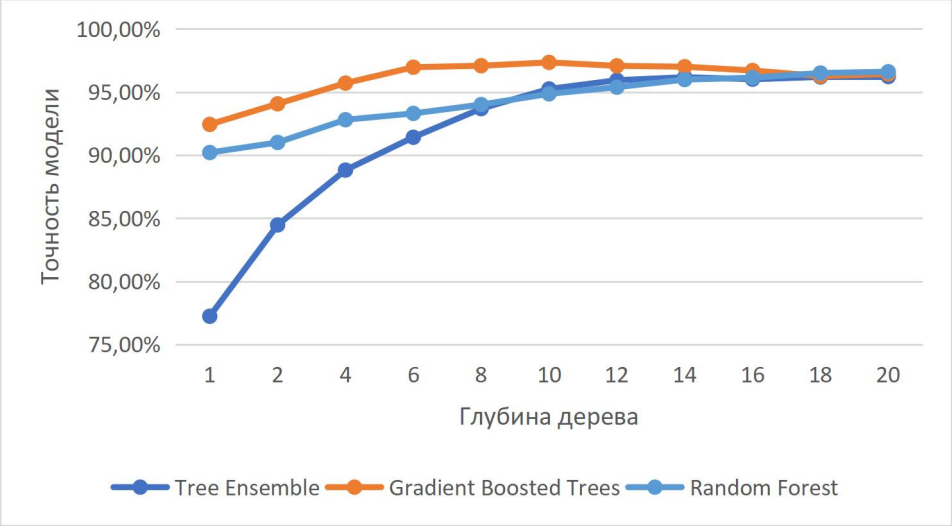

Рисунок 3 - Обобщающий график результатов.

Ансамблевые методы (Random Forest, GBM, Tree Ensemble) показали лучшие результаты благодаря:

1. Способности анализировать сложные нелинейные зависимости в данных.
2. Устойчивости к переобучению за счет бэггинга/бустинга.
3. Автоматическому отбору значимых признаков, что критично для задач с множеством параметров.

4. Вывод

Исследование показывает, что использование машинного обучения в обнаружении потенциально опасных сайтов и детектировании фишинговых атак перспективно, потому что обучение и дальнейшее использование искусственного интеллекта позволит развивать данную сферу, создавая и усовершенствуя модели машинного обучения, позволяя им быстрее и точнее находить закономерности в параметрах и прогнозировать легитимность сайтов, писем и уведомлений [16]

5. Благодарность

Исследование выполнено за счет гранта Российского научного фонда № 25-71-30007, https://rscf.ru/project/25-71-30007/

6. Список литературы

[1] Завьялов Александр Николаевич Интернет-Мошенничество (Фишинг): Проблемы Противодействия и Предупреждения // Baikal Research Journal. 2022. №2. URL: https://brj-bguep.ru/reader/article.aspx?id=25141

[2] History of Phishing // Phishing URL: https://www.phishing.org/history-of-phishing

[3] Cisco. Целевой фишинг. // ТЕХНО Н URL: https://technon.ru/upload/pdf/ironport_targeted_phishing.pdf

[4] Афанасьева Н. С., Елизаров Д. А., Мызникова Т. А. Классификация фишинговых атак и меры противодействия им //Инженерный вестник Дона. – 2022. – №. 5 (89). – С. 169-182.

[5] Фишинговые письма: как их распознать и не стать их жертвой // Kaspersky URL: https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips

[6] Как работает фишинг через поисковые системы? // keeper URL: https://www.keepersecurity.com/blog/ru/2023/04/12/what-is-search-engine-phishing/

[7] Making the world’s information safely accessible // Google Safe Browsing URL: https://safebrowsing.google.com
[8] Here’s why people are saying two-factor authentication isn’t perfect // Digitaltrends URL: https://www.digitaltrends.com/computing/why-two-factor-authentication-isnt-perfect/
[9] Корнюхина С. П., Лапонина О. Р. Исследование возможностей алгоритмов глубокого обучения для защиты от фишинговых атак //International Journal of Open Information Technologies. – 2023. – Т. 11. – №. 6. – С. 163-174.
[10] Boyle P., Shepherd L. A. Mailtrout: a machine learning browser extension for detecting phishing emails //34th British HCI Conference. – BCS Learning & Development, 2021. – С. 104-115.
[11] CyberSecurity : BookMyShow ads URL Analysis // kaggle URL: https://www.kaggle.com/datasets/shibumohapatra/book-my-show
[12] KNIME Analytics Platform // KNIME URL: https://www.knime.com/knime-analytics-platform
[13] Biau G., Scornet E. A random forest guided tour //Test. – 2016. – Т. 25. – №. 2. – С. 197-227.
[14] Natekin A., Knoll A. Gradient boosting machines, a tutorial //Frontiers in neurorobotics. – 2013. – Т. 7. – С. 21.
[15] Асито Ф. Предсказательная аналитика с KNIME / пер. с англ. А. Ю. Гинько. – М.: ДМК Пресс, 2025. – 360 с.: ил.
[16] Отахонов А. А. Обнаружение и оценка фишинговых url-адресов с использованием алгоритмов машинного обучения //Al-Farg’oniy avlodlari. – 2024. – №. 4. – С. 382-390.