15. *Kanojiya R.G., Meshram P.M.* Optimal tuning of PI controller for speed control of DC motor drive using particle swarm optimization, *2012 International Conference on Advances in Power Conversion and Energy Technologies (APCET)*, 2012.
16. *Kamal M., Mathew L., Chatterji S.* Speed control of brushless DC motor using intelligent controllers, *2014 Students Conference on Engineering and Systems*, 2014.
17. *Meena D., Chauhan S.* Speed control of DC servo motor using genetic algorithm, *2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, 2017.
18. *Mishra P., [et al.]*. Optimization of PID Controller with First Order Noise Filter, *2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, 2015.
19. *Kravchenko Yu.A.* Postroenie prognoznykh modeley dinamicheskikh sistem na osnove integratsii neyronnykh setey i geneticheskikh algoritmov [Construction of predictive models of dynamic systems based on the integration of neural networks and genetic algorithms], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2006, Vol. 64, No. 9-1, pp. 103-104.
20. *Gladkov L.A., Kureychik V.V., Kureychik V.M.* Geneticheskie algoritmy [Genetic algorithms], 2010.

Ахмад Зулфикар – Московский государственный технологический университет “Станкин”; e-mail: zoualfikarahmad@gmail.com; г. Москва, Россия; тел.: +79636898784; кафедра компьютерных систем управления; аспирант.

Кравченко Юрий Алексеевич – Южный федеральный университет; e-mail: yakravchenko@sfedu.ru; г. Таганрог, Россия; тел.: +79289080151; кафедра систем автоматизированного проектирования им. В.М. Курейчика; профессор.

Мансур Али Махмуд – Южный федеральный университет; e-mail: mansur@sfedu.com; г. Таганрог, Россия; тел.: +79880158697; кафедра систем автоматизированного проектирования им. В.М. Курейчика; программист.

Ahmad Zoualfikar – Moscow State Technological University "Stankin"; e-mail: zoualfikarahmad@gmail.com; Moscow, Russia; phone: +79636898784; the Department of Computer Control Systems; postgraduate student.

Kravchenko Yury Alekseevich – Southern Federal University; e-mail: yakravchenko@sfedu.ru; Taganrog, Russia; phone: +79289080151; the Department of Computer Aided Design named after V.M. Kureichik; professor.

Mansour Ali Mahmoud – Southern Federal University; e-mail: mansur@sfedu.com; Taganrog, Russia; phone: +79880158697; the Department of Computer Aided Design named after V.M. Kureichik; programmer.

УДК 004.89 DOI 10.18522/2311-3103-2025-4-250-262

М.А. Лапина, Д.А. Лукьянов, В.Г. Лапин, Н.Н. Кучеров

ИССЛЕДОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ САЙТОВ-МОШЕННИКОВ

В настоящее время большое количество процессов связано с большими объёмами данных, которые необходимо анализировать. С увеличением объёма информации её анализ становится более объёмной и сложной задачей. Возникает проблема поиска инструмента, который поможет компаниям и учреждениям в сборе, анализе и прогнозировании данных. Машинное обучение является областью искусственного интеллекта, которая находит закономерности в базе данных и на их основе пытается спрогнозировать результат. Ещё одной областью применения машинного обучения является детектирование сайтов-мошенников. 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. Исследование направлено на систематизацию знаний о фишинговых атаках и исследовании методов машинного обучения для обнаружения сайтов-мошенников. 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. Анализ данных, предоставленных в датасете, позволил преобразовать данные для корректной работы моделей, что позволило избежать ошибок. Была решена проблема переобучения моделей машинного обучения. Детальное изучения датасета позволило отфильтровать данные, которые могли

вызывать ошибки в работе модели и понизить качество прогнозирования. 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. Был проведён анализ исследования и подведены результаты проведённой работы.

Машинное обучения; фишинг; сайт-мошенник; KNIME; киберпреступность; кибер-атаки; поиск уязвимостей; искусственный интеллект.

M.A. Lapina, D.A. Lukyanov, V.G. Lapin, N.N. Kucherov

RESEARCH OF MACHINE LEARNING METHODS FOR DETECTING FRAUDULENT WEBSITES

Every year our lives become more and more connected with large volumes of data that need to be analyzed. As the volume of information increases, its analysis becomes a more voluminous and complex task. In this situation, the problem of finding a tool that will help companies and institutions in collecting, analyzing and forecasting data arises. Machine learning is an area of artificial intelligence that finds patterns in a database and, based on them, tries to predict the result. Another area of application of machine learning is the detection of fraudulent sites. Currently, with the development of information technology, digital crimes have become a serious threat to confidential information and user data. Artificial intelligence is able to analyze site parameters and determine the presence of threats to information. The study is aimed at systematizing knowledge about phishing attacks and studying machine learning methods for detecting fraudulent sites. During the study, machine learning methods for detecting phishing sites were developed, schemes were built that allow machine learning models to correctly transform data for feeding them to models. The analysis of the data provided in the dataset made it possible to correctly transform the data for the correct operation of the models, which will avoid errors. The problem of retraining machine learning models was solved. A detailed study of the dataset made it possible to filter out data that could cause errors in the model and reduce the quality of artificial learning forecasting. As a result of the work, the developed methods for searching for phishing attacks using machine learning models were tested on test data, based on the results obtained, graphs of changes in the accuracy of detecting illegitimate sites from changing the model settings were constructed. An analysis of the study was carried out and the results of the work were summarized.

Machine learning; phishing; fraudulent website; KNIME; cybercrime; cyber attacks; vulnerability scanning; artificial intelligence.

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. Хакеры создают копии оригинальных сайтов, которые внешне трудно отличить от легитимных. Вводя персональные данные, пользователь передаёт их в руки злоумышленникам, которые смогут активно пользоваться почтой, банковской картой или паспортными данными объекта атаки. Впервые методы, которые используют современные хакеры, были описаны в 1987 году [2]. 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. Суть атаки заключалась в использовании злоумышленниками алгоритмов для генерации случайных номеров кредитных карт и регистрации их в системе AOL (America online), позже они использовались для рассылки спама. Хакеры маскировались под сотрудников AOL и просили пользователей обновить их данные: пароли, банковские счета. Позже данные попадали к злоумышленникам [3]. Общий план фишинговой атаки проиллюстрирована на рис. 1.

С развитием технологий хакеры придумывают новые способы, с помощью которых проводятся фишинговые атаки. В 2003 году была зарегистрирована первая фишинговая атака на банк о чем банк The Banker сообщил в статье Криса Сангани под названием“ Борьба с кражей личных данных” [4, 5].

В 2007 году 3,6 миллиона человек потеряли в общей сумме 3,2 миллиарда долларов США в результате фишинговых атак. Хакеры использовали навыки социальной инженерии, отправляя на почту пользователей открытки с поздравлениями, купоны на скидку и письма от технической поддержки сайта [6].

Рис. 1. План фишинговой атаки

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 – вид фишинга, для которого злоумышленники используют письма, приходящие на почту пользователей. Этот вид атак имеет специализированный подход, благодаря социальным сетям, злоумышленники собирают информацию о пользователе. Собранную информацию хакеры используют в письме, убеждая получателя в том, что письмо отправлено кем-то другим в организации. В итоге, злоумышленники заполучают доступ к данным пользователя [7].

Vishing – данный вид фишинговой атаки основан на использовании телефонного звонка. Пользователю поступают звонки от злоумышленников, которые получают информацию манипуляциями. Данная атака построена на создании у пользователя ощущения критичности и срочности, чтобы у него не осталось другого выхода, кроме как передать конфиденциальные данные в руки преступников [8].

Клон-фишинг – в данном виде фишинга также используется электронная почта. Злоумышленники создают точную копию письма, которое уже получал пользователь, меня в них ссылки и вложения. Пользователь, не подозревая обмана, открывает данное письмо, передавая данные преступникам [9].

Фишинг в поисковых системах – данный вид фишинга основан на обходе фильтров поисковых систем. Хакеры используют SEO (поисковую оптимизацию), чтобы их сайт стоял в поиске выше других и больше пользователей перешли на фишинговый сайт. Данные сайты являются клонами-двойниками оригинальных сайтов. Пользователи вводят свои данные, которые переходят в руки мошенников [10].

В табл. 1 приведены существующих в настоящее время способы защиты данных от фишинговых атак.

Таблица 1

Сравнительный анализ методов защиты от фишинговых атак

Методы	Характеристики				
	Удобность	Конфиденциальность	Доступность	Приватность	Целостность
Фильтрация URL [11]	✔		✔		✔
Двухфакторная аутентификация [12]		✔	✔	✔	✔
Обучение пользователей [13]		✔	✔	✔	
Браузерные расширения [14]	✔		✔		

На основе приведённой таблицы можно сделать вывод, что в настоящее время универсального способа гарантированно защититься от фишинговых атак нет, каждый из методов используется преимущественно для блокирования или детектирования отдель-

ных видов фишинговых атак, но активное развитие машинного обучения позволяет облегчить поиск потенциально опасных сайтов, ссылок и писем, которые могут быть разработаны хакерами.

Ожидаемыми результатами исследования являются:

1) Систематизация слабостей и уязвимостей систем перед фишинговыми атаками.

2) Изучение и создание методов машинного обучения для детектирования фишинговых сайтов.

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) [15], в котором внесены основные характеристики сайтов и результат. Данный датасет создан для обнаружения фишинговых сайтов, которые маскируются под легитимными ресурсами, чтобы украсть данные пользователей. Используя машинное обучение, можно обучать модели машинного обучения анализировать параметры сайтов и находить в них закономерности, которые помогут определить легитимность сайта. Для более детальной и точной работы с датасетом необходимо произвести анализ: определить типы данных, разбить данные на более важные и менее важные для машинного обучения.

Для обнаружения сайтов-мошенников необходимо предоставить модели машинного обучения параметры, которые будут анализироваться и проверяться. Параметры, необходимые для проверки сайта на легитимность представлены на рис. 2.

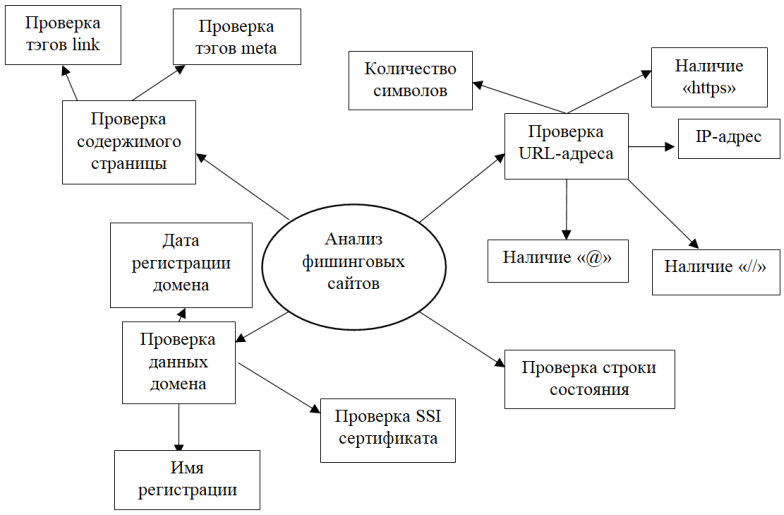

Рис. 2. Параметры, анализируемые при поиске фишинговых сайтов

Размер и структура: данный датасет [15] содержит в себе 11055 строк и 32 столбца. Один столбец index содержит категориальные данные, остальные 31-числовые.

Целевая переменная: целевым столбцом является столбец Result, в нём содержится две переменные (0 и 1).

Характеристика признаков: столбцы представляют собой бинарные и категориальные признаки (-1,0,1). Некоторые признаки связаны с URL-адресами (URLURL_Length). Другие относятся к характеристикам страницы (Page_Rank). Так же наблюдаются признаки, касающиеся безопасности (statistical_report).

Важность признаков: данные можно разбить на три группы важности для машинного обучения: ключевые для модели, средней важности и менее значимые.

К ключевым для модели данным относятся: having_IPhaving_IP_address, SSLfinal_State, web_traffic, Google_Index, Page_Rank, age_of_domain, DNSRecord.

К средней важности относятся: having_sub_domain, Prefix_Suffix, Shortining_Servicce, Reauest_URL.

К менее важным можно отнести следующие столбцы: popUpWindow, on_mouseover, RightClick, Iframe.

На основе полученных данных из анализа датасета и основываясь на информацию рис. 3, необходимо произвести выборку основных параметров, которые модель машинного обучения будет анализировать и на их основе прогнозировать результат проверки легитимности сайтов.

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 [16].

KNIME [16] – это аналитическая платформа с удобным интерфейсом, предназначенная для работы с моделями машинного обучения, анализа и обработки данных и автоматизации процессов аналитики. Платформа позволяет пользоваться машинным обучением, не используя языки программирования, все необходимые команды уже запрограммированы в специальные узлы (Nodes), которые и выполняют основные функции в чтении, обработке, анализе, прогнозировании и визуализации данных. Данная платформа предоставляет широкий выбор моделей машинного обучения. Использованные в исследовании модели представлены на рис. 3.

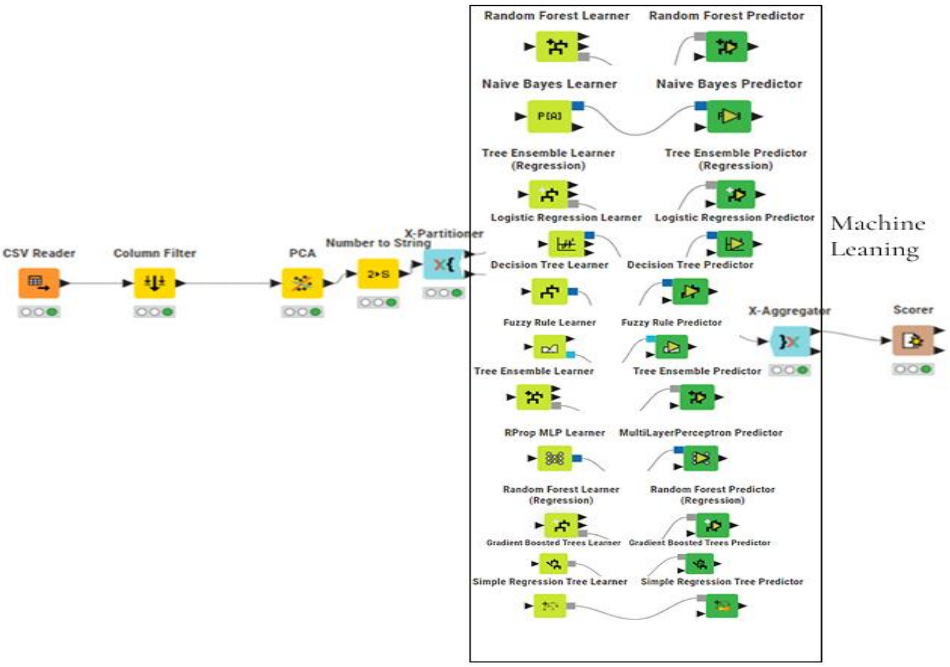

Рис. 3. Модели машинного обучения

Данные модели машинного обучения являются одними из самых популярных. Для использования предоставляются следующие модели: деревья решений, ансамбли деревьев решений, случайные леса деревьев решений, логическая регрессия, линейная регрессия, нейронные сети, метод к-ближайших соседей, обучение решением последовательных задач, наивный байес, модель, использующая нечёткую логику для обучения.

В данном исследовании поставлена задача классификации, присвоение сайтам категорий: 1– сайт фишинговый, 0 – сайт легитимный.

Для решения поставленной задачи была собрана схема, позволяющая загрузить данные датасета в модель машинного обучения Decision Tree Learner. Первым шагом было создание рабочего места (Workflow), воспользовавшись узлом необходимо считать данные датасета (Node) CSV Reader (IO → Read → CSV Reader), необходимо выбрать путь до файла. В данном виде в Decision Tree Learner подавать данные нельзя, необходимо преобразовать их перед дальнейшим обучением модели. Для этого воспользуемся узлами: Column filter (Manipulation → column → column filter), PCA (Analytics → PCA), Number to String (Manipulation → convert & replace). После преобразования данных их необходимо разделить на две составляющие: обучающие данные, которые пойдут на обучение модели машинного обучения и тестовые, на которых обученная модель будет тестироваться, для этого необходимо использовать узел (Node) X-Partitioner (Analytics → cross validation → X-Partitioner). Данная нода в связи с нодой X-Aggregator позволяет пользоваться такой функцией как кросс-валидация. Нода Decision Tree Learner (Analytics → Decision Tree → Decision Tree Learner) является узлом, который является обучающей моделью машинного обучения. Данный узел имеет код, позволяющий машине использовать метод деревьев решений для обнаружения закономерности в параметрах легитимных и фишинговых сайтах. Decision Tree Predictro (Analytics → Decision Tree → Decision Tree Predictor) нода, позволяющая обученной модели использовать тестовые данные для прогнозирования легитимности сайтов. Нода Scorer (Analytics → Scoring → Scorer) является узлом, который позволяет оценивать точность спрогнозированных моделью данных, строить матрицу ошибок, позволяющая оценить, где были допущены ошибки при обучении модели [17]. Данная схема является обобщающей схемой модели машинного обучения, в дальнейшем исследовании будут использованы модели, показанные на рис. 3, которые показывали наилучший результат.

Модели машинного обучения. Каждая модель машинного обучения применяется в разных областях, для разных целей, классификация данные подразумевает использование всех существующих моделей машинного обучения. Для более широкого понимания в каком аспекте одна модель будет лучше другой создана сравнительная таблица (табл. 2) с характеристиками всех использованных моделей.

Таблица 2

Сравнительный анализ моделей машинного обучения

Модели МО	Характеристики			
	Производительность	Интерпретируемость	Устойчивость	Универсальность
Decision Tree [17]		✔		✔
RProp MLP [16] [17]			✔	✔
Naïve Bayes [16] [17]	✔	✔		
Random Forest [16]		✔	✔	✔
DL [17]			✔	✔
Logistic Regression [16] [17]	✔	✔		✔
Tree Ensemble [17]		✔	✔	✔
PNN [17]			✔	✔
Fuzzy Rule [17]	✔	✔		
Tree Ensemble(Regression) [17]		✔	✔	✔

В исследовании были использованы модели, использующие деревья решений для классификации. Для более детального и полного понимания принципа работы алгоритма необходимо математически обосновать использование данного метода в решении задачи классификации.

Деревья решений – модель машинного обучения, использующаяся для регрессии и классификации путём разбиения пространства признаков на области, соответствующие целевым значениям. Выделяют следующие этапы работы деревьев решений:

Структура деревьев.

Деревья состоят из **узлов**, в которых происходит проверка условий, **листьев**, которые содержат итоговые предсказания.

Разбиение пространства признаков.

На каждом узле дерево выбирает **признак** x_j и **порог** t, чтобы разделить данные на две подгруппы:

$$\text{Левые потомки: } \{x|x_j \le t\}, \text{Правые потомки } \{x|x_j > t\}$$

Оптимизация.

Выбор наилучшего разбиения основан на максимальной информативности. Для этого в деревьях решений используются:

Энтропия

$$H(D) = -\sum_{k=1}^{K} p_k \log_2 p_k, p_k = \frac{|D_k|}{|D|}$$

Индекс Джини

$$G(D) = 1 - \sum_{k=1}^{K} p_k^2$$

Прирост информации

$$IG = H(D) - \sum_{s\in\{left,right\}} \frac{|D_s|}{|D|} H(D_s)$$

4. Формальное предсказание:

Для нового элемента x дерево проходит путь от корня до листа, применяя условия узла. Предсказание высчитывается следующим образом,

$$f(x) = \sum_{m=1}^{M} c_m \cdot I(x \in R_m),$$

где R_m – область, соответствующая m-му листу, c_m – его значение, I – индикаторная функция

1) Модель машинного обучения **Random Forest** используется в своём алгоритме принцип деревьев решения, которые разделяют данные на основе признаков, искусственный интеллект создаёт лес деревьев решения и высчитывает среднее значение точности всех деревьев. Данная модель используется для классификации и регрессии.

На основе проведённых испытаний модели по обнаружению фишинговых атак построен график (рис. 4), демонстрирующий точность модели от её настроек.

Таблица 3

Точность модели

Tree depth	Accuracy, %
1	90.20
2	91.00
4	92.80
6	93.30
8	94.00
10	94.85
12	95.38
14	95.98
16	96.13
18	96.50
20	96.60

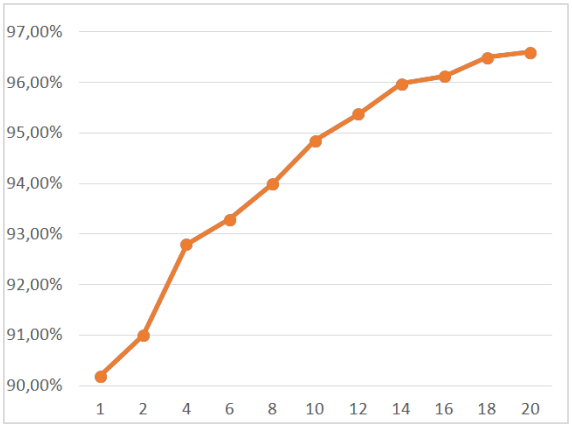

Рис. 4. График изменения точности модели

2) Модель машинного обучения **Tree Ensemble** использует ансамбль деревьев, каждое дерево прогнозирует данные, после прогнозирования прогнозы объединяются. Данная модель используется для классификации и регрессии. На основе проведённых испытаний модели построен график (рис. 5), который демонстрирует точность модели.

Таблица 4

Точность модели

Tree depth	Accuracy, %
1	89.04
2	90.77
4	92.83
6	92.96
8	93.85
10	94.56
12	95.44
14	95.92
16	96.21
18	96.32
20	96.59

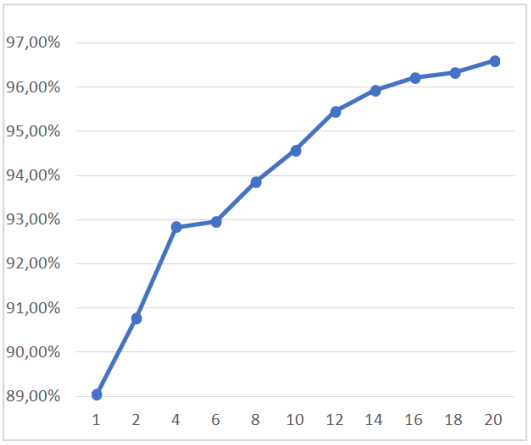

Рис. 5. График изменения точности модели

3) Модель машинного обучения **PNN** – алгоритм, который использует обучение на множестве последовательных задач, сохраняя данные из предыдущих задач.

На основе проведённых испытаний модели построен график (рис. 6), который демонстрирует точность модели.

Таблица 5

Точность модели

Theta minus(Plus)	Accuracy
0.1	87,50%
0.2	87,09%
0.3	86,40%
0.4	86,27%
0.5	86,59%
0.6	86,16%
0.7	82,91%
0.8	70,20%
0.9	55,71%
1	-

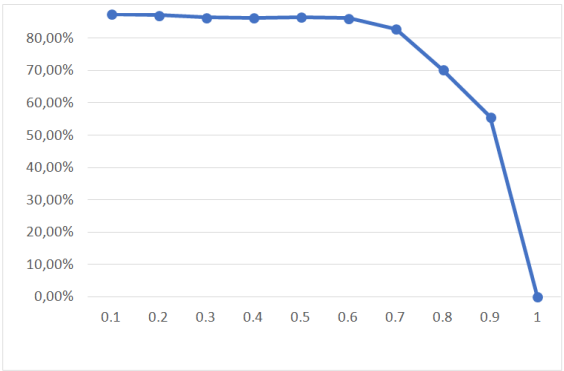

Рис. 6. График изменения точности модели

4) Модель машинного обучения **Gradient Boosted Trees** – данная модель использует алгоритм градиентного спуска для деревьев решений, что позволяет минимизировать потери точности.

На основе результатов проведённого исследования был построен график, представленный на рис. 7.

Таблица 6

Точность модели

Tree depth	Accuracy,%
1	92.43
2	94.06
4	95.70
6	96.96
8	97.08
10	97.34
12	97.07
14	97.00
16	96.70
18	96.26
20	96.42

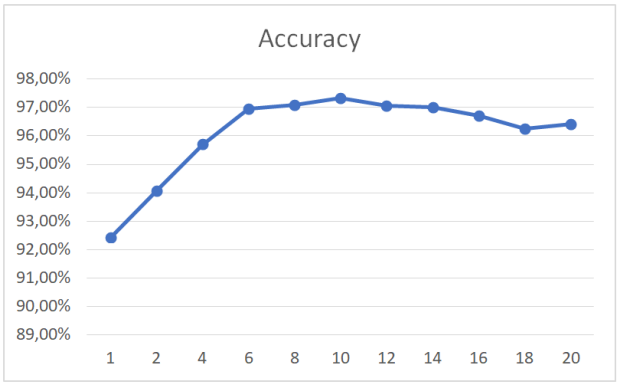

Рис. 7. График изменения точности модели

5) Модель машинного обучения **Tree Ensemble** – данная модель использует деревья решений для регрессии, что помогает классифицировать легитимные и фишинговые сайты. На основе результатов проведённого исследования был построен график, представленный на рис. 8.

Таблица 7

Точность модели

Tree depth	Accuracy,%
1	77,23%
2	84,46%
4	88,81%
6	91,41%
8	93,68%
10	95,24%
12	95,93%
14	96,17%
16	96,01%
18	96,19%
20	96,22%

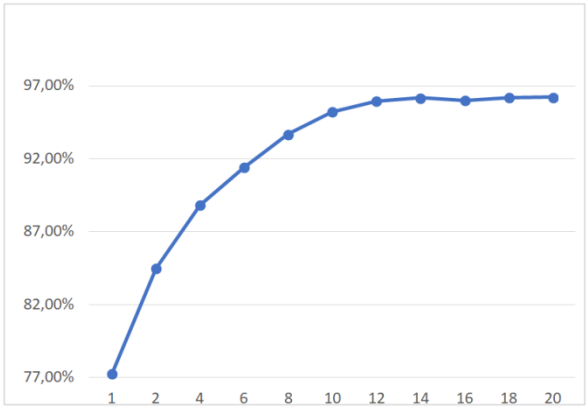

Рис. 8. График изменения точности модели

На основе проведённых испытаний был построен обобщающий график (рис. 9), включающий в себя результаты работы всех моделей машинного обучения.

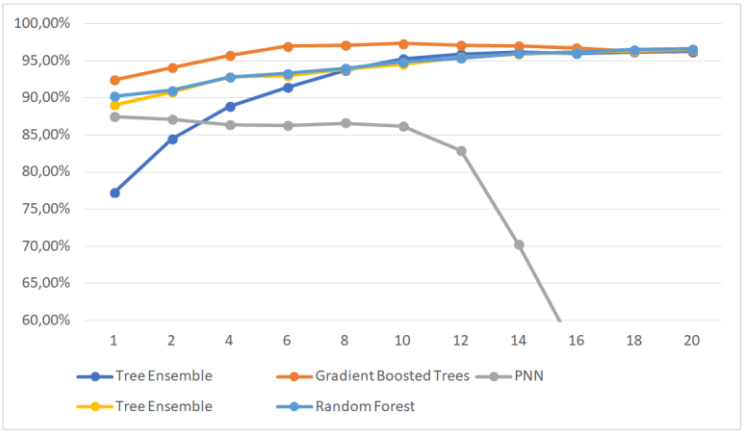

Рис. 9. Обобщающий график результатов

Борьба с переобучением. При проведении испытаний моделей машинного обучения была обнаружена проблема переобучения искусственного интеллекта, когда модель запоминает обученные данные и показывает 100% точность тестирования. Данная проблема критична и нуждается в решении по той причине, что, загрузив абсолютно новые данные, модель машинного обучение не сможет правильно обучиться и спрогнозировать результат. В данном исследовании решением проблемы переобучения модели является кросс-валидация. Кросс-валидация позволяет разделить вводимые данные на равные части, каждая часть данных будет обучающей и тестируемой, что позволит машине обучаться и проводить тестирование на абсолютно новых данных. В KNIME данная функция реализуется благодаря двум узлам (X-partitioner и X-aggregator) (рис. 10). В узле X-partitioner выставляется колонка, которую нода будет разделять на равные части и выбирается число циклов, которое пройдут данные перед их оцениванием. X-aggregator позволяет запустить цикл вновь, подавая на обучение новую часть данных. Использование данных узлов, помогло справиться с проблемой переобучения модели машинного обучения, что позволило создать исследование более точным и достоверным.

Рис. 10. Кросс-валидация

Заключение. На данный момент наблюдается рост преступлений совершённых с помощью информационных технологий. Почти 50% преступлений в данной сфере приходятся на взлом кодов от банковских карт населения, которые злоумышленники совершают с помощью фишинговых атак. Существующие методы защиты от фишинга не всегда справляется с детектированием угрозы. Использование машинного обучения в перспективе может помочь специалистам в сфере информационной безопасности и компаниям фильтровать потенциально фишинговые сайты, письма и уведомления [19].

Проведённое исследование демонстрирует изобретательность злоумышленников в создании новых методов фишинговых атак, обнаружение которых становится более трудной и долгой задачей для стандартных методов детектирования фишинга. Испытания, проведённые с моделями машинного обучения, показывают высокие результаты точности обнаружения фишинговых сайтов. Тестирование искусственного интеллекта показывает, что модели способны выдавать высокую точность, охватывая полный объём данных, вводимый в модель.

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 [20].

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

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Завьялов А.Н.* Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. – 2022. – Т. 13, № 2. – URL: https://brj-bguep.ru/reader/article.aspx?id=25141 (дата обращения: 28.03.2025).
2. History of Phishing // Phishing. – URL: https://www.phishing.org/history-of-phishing (дата обращения: 28.03.25).
3. *Данько О.С., Медведева Т.А.* Исследование техник фишинга и методов защиты от него // Молодой исследователь Дона. – 2021. – № 3 (30). – С. 60-61.
4. *Gupta B.B., Tewari A., Jain A.K. et al.* Fighting against phishing attacks: state of the art and future challenges // Neural Comput & Applic. – 2017. – 28. – P. 3629-3654. – https://doi.org/10.1007/s00521-016-2275-y (дата обращения: 28.03.2025).
5. *Сангани Крис*. Борьба с кражей личных данных // The Banker. – Сентябрь 2003. – 70 (9). – 5354. – URL: https://www.thebanker.com/content/fc6f8422-54f4-5641-a89d-607d895fe7cc.
6. *McCall Tom.* (December 17, 2007). Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks // Gartner. Archived from the original on November 18, 2012. Retrieved December 20, 2007. – URL: https://web.archive.org/web/20121118162442/http://www.gartner.com/it/page.jsp?id=565125.
7. Cisco. Целевой фишинг // ТЕХНО Н. – URL: https://technon.ru/upload/pdf/ironport_targeted_phishing.pdf (дата обращения: 28.03.2025).
8. *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.
9. Фишинговые письма: как их распознать и не стать их жертвой // Kaspersky. – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips (дата обращения: 28.03.2025).
10. Как работает фишинг через поисковые системы? // keeper. – URL: https://www.keepersecurity.com/blog/ru/2023/04/12/what-is-search-engine-phishing/ (дата обращения: 28.03.2025).
11. Making the world’s information safely accessible // Google Safe Browsing. – URL: https://safebrowsing.google.com (дата обращения: 29.03.2025).
12. 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/ (дата обращения: 29.03.2025).
13. *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.
14. *Boyle P., Shepherd L.A.* Mailtrout: a machine learning browser extension for detecting phishing emails // 34th British HCI Conference. – BCS Learning & Development, 2021. – P. 104-115.
15. CyberSecurity: BookMyShow ads. – URL Analysis // kaggle. – URL: https://www.kaggle.com/datasets/shibumohapatra/book-my-show (дата обращения: 04.04.2025).
16. KNIME Analytics Platform // KNIME. – URL: https://www.knime.com/knime-analytics-platform (дата обращения: 04.04.2025).
17. *Асито Ф.* Предсказательная аналитика с KNIME: пер. с англ. А.Ю. Гинько. – М.: ДМК Пресс, 2025. – 360 с.
18. *Боровиков М.М.* Проблемы противодействия транснациональным преступным сообществам в условиях трансформирующегося мира // Экономика, финансы, проектное управление и социальная система России: подходы и перспективы в условиях устойчивого цифрового развития. Краснодар, 20 мая 2022 года. – URL: https://krasnodar.fa.ru/upload/constructor/a74/jr1ym9fbu4a1p6dq3me0z4do0s700f41.pdf.
19. *Антонова Т.С., Смирнов В.М.* Фишинг как неизученное киберпреступление // StudNet. – 2021. – Т. 4, №. 6. – С. 69-75.
20. *Отахонов А.А.* Обнаружение и оценка фишинговых url-адресов с использованием алгоритмов машинного обучения // Al-Farg’oniy avlodlari. – 2024. – № 4. – С. 382-390.

REFERENCES

1. *Zav'yalov A.N.* Internet-moshennichestvo (fishing): problemy protivodeystviya i preduprezhdeniya [Internet fraud (phishing): problems of counteraction and prevention], *Baikal Research Journal*, 2022, Vol. 13, No. 2. Available at: https://brj-bguep.ru/reader/article.aspx?id=25141 (accessed 28 March 2025).
2. History of Phishing, *Phishing*. Available at: https://www.phishing.org/history-of-phishing (accessed 28 March 2025).
3. *Dan'ko O.S., Medvedeva T.A.* Issledovanie tekhnik fishinga i metodov zashchity ot nego [Research of phishing techniques and methods of protection against it], *Molodoy issledovatel' Dona* [Young researcher of the Don], 2021, No. 3 (30), pp. 60-61.
4. *Gupta B.B., Tewari A., Jain A.K. et al.* Fighting against phishing attacks: state of the art and future challenges, *Neural Comput & Applic*., 2017, 28, pp. 3629-3654. Available at: https://doi.org/10.1007/s00521-016-2275-y (accessed 28 March 2025).
5. *Sangani Kris.* Bor'ba s krazhey lichnykh dannykh [Fighting identity theft], *The Banker*, Sentyabr' 2003, 70 (9), 5354. Available at: https://www.thebanker.com/content/fc6f8422-54f4-5641-a89d-607d895fe7cc.
6. *McCall Tom.* (December 17, 2007). Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks, *Gartner*. *Archived from the original on November 18, 2012. Retrieved December 20, 2007*. Available at: https://web.archive.org/web/20121118162442/http://www.gartner.com/it/page.jsp?id=565125.
7. Cisco. TSelevoy fishing [Cisco. Spear phishing], *TEKhNO N* [TECHNO N]. Available at: https://technon.ru/upload/pdf/ironport_targeted_phishing.pdf (accessed 28 March 2025).
8. *Afanas'eva N.S., Elizarov D.A., Myznikova T.A.* Klassifikatsiya fishingovykh atak i mery protivodeystviya im [Classification of phishing attacks and countermeasures], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2022, No. 5 (89), pp. 169-182.
9. Fishingovye pis'ma: kak ikh raspoznat' i ne stat' ikh zhertvoy [Phishing emails: how to recognize them and avoid becoming their victim], *Kaspersky*. Available at: https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips (accessed 28 March 2025).
10. Kak rabotaet fishing cherez poiskovye sistemy? [How does phishing through search engines work?], *keeper*. Available at: https://www.keepersecurity.com/blog/ru/2023/04/12/what-is-search-engine-phishing/ (accessed 28 March 2025).
11. Making the world's information safely accessible, *Google Safe Browsing*. Available at: https://safebrowsing.google.com (accessed 28 March 2025).
12. Here's why people are saying two-factor authentication isn't perfect, *Digitaltrends*. Available at: https://www.digitaltrends.com/computing/why-two-factor-authentication-isnt-perfect/ (accessed 28 March 2025).
13. *Kornyukhina S.P., Laponina O.R.* Issledovanie vozmozhnostey algoritmov glubokogo obucheniya dlya zashchity ot fishingovykh atak [Study of the capabilities of deep learning algorithms for protection against phishing attacks], *International Journal of Open Information Technologies*, 2023, Vol. 11, No. 6, pp. 163-174.
14. *Boyle P., Shepherd L.A.* Mailtrout: a machine learning browser extension for detecting phishing emails, *34th British HCI Conference*. BCS Learning & Development, 2021, pp. 104-115.
15. CyberSecurity: BookMyShow ads. URL Analysis, *kaggle*. Available at: https://www.kaggle.com/datasets/shibumohapatra/book-my-show (accessed 04 April 2025).
16. KNIME Analytics Platform, *KNIME*. Available at: https://www.knime.com/knime-analytics-platform (accessed 04 April 2025).
17. *Asito F.* Predskazatel'naya analitika s KNIME [Predictive analytics with KNIME transl. from engl. by A.Yu. Gin'ko. Moscow: DMK Press, 2025, 360 p.
18. *Borovikov M.M.* Problemy protivodeystviya transnatsional'nym prestupnym soobshchestvam v usloviyakh transformiruyushchegosya mira [Problems of counteracting transnational criminal communities in the context of a transforming world], *Ekonomika, finansy, proektnoe upravlenie i sotsial'naya sistema Rossii: podkhody i perspektivy v usloviyakh ustoychivogo tsifrovogo razvitiya* [Economy, finance, project management and the social system of Russia: approaches and prospects in the context of sustainable digital development]. Krasnodar, 20 May 2022. Available at: https://krasnodar.fa.ru/upload/constructor/a74/jr1ym9fbu4a1p6dq3me0z4do0s700f41.pdf.
19. *Antonova T.S., Smirnov V.M.* Fishing kak neizuchennoe kiberprestuplenie [Phishing as an unexplored cybercrime], *student*, 2021, Vol. 4, No. 6, pp. 69-75.
20. *Otakhonov A.A.* Obnaruzhenie i otsenka fishingovykh url-adresov s ispol'zovaniem algoritmov mashinnogo obucheniya [Detection and evaluation of phishing URLs using machine learning algorithms], *Al-Farg'oniy avlodlari,* 2024, No. 4, pp. 382-390.

Лапина Мария Анатольевна – Северо-Кавказский федеральный университет; e-mail: mlapina@ncfu.ru; г. Ставрополь, Россия; к.ф.-м.н.; доцент кафедры вычислительной математики и кибернетики; ORCID: 0000-0001-8117-9142.

Лукьянов Дмитрий Александрович – Северо-Кавказский федеральный университет; e-mail: ilia.alekseev.kenig@gmail.com; г. Ставрополь, Россия; кафедра вычислительной математики и кибернетики; студент; ORCID: 0009-0009-7203-0309.

Лапин Виталий Геннадьевич – Северо-Кавказский федеральный университет; e-mail: vitlx@yandex.ru; г. Ставрополь, Россия; к.ф.-м.н.; доцент кафедры вычислительной математики и кибернетики; ORCID: 0000-0002-0611-7002.

Кучеров Николай Николаевич – Северо-Кавказский федеральный университет; e-mail: nik.bekesh@gmail.com; г. Ставрополь, Россия; к.т.н.; ведущий научный сотрудник департамента науки СКФУ; ORCID: 0000-0003-0337-0093.

Lapina Maria Anatolyevna – North Caucasus Federal University; e-mail: mlapina@ncfu.ru; Stavropol, Russia; cand. of phys. and math. sc.; associate professor of the Department of Computational Mathematics and Cybernetics; ORCID: 0000-0001-8117-9142.

Lukyanov Dmitry Alexandrovich – North Caucasus Federal University; e-mail: ilia.alekseev.kenig@gmail.com; Stavropol, Russia; the Department of Computational Mathematics and Cybernetics; ORCID: 0009-0009-7203-0309.

Lapin Vitalii Gennadievich – North Caucasus Federal University; e-mail: vitlx@yandex.ru; Stavropol, Russia; cand. of phys. and math. sc.; associate professor of the Department of Computational Mathematics and Cybernetics; ORCID: 0000-0002-0611-7002.

Kucherov Nikolay Nikolaevich – North Caucasus Federal University; e-mail: nik.bekesh@gmail.com; Stavropol, Russia; cand. of eng. sc.; leading researcher of the Department of Science; ORCID: 0000-0003-0337-0093.

УДК 007.52:004.81:339.37 DOI 10.18522/2311-3103-2025-4-262-272

М.А. Хапова, К.Ч. Бжихатлов, Л.Б. Кокова

РАЗРАБОТКА АВТОНОМНОГО РОБОТА ДЛЯ ВЫПОЛНЕНИЯ ФУНКЦИЙ ПРОДАВЦА - КОНСУЛЬТАНТА В СЕТЯХ РОЗНИЧНОЙ ТОРГОВЛИ

Активное увеличение доли крупных сетевых магазинов в торговом секторе повышает спрос на сотрудников подобных сетей. При этом, с ростом оборота крупных магазинов растут и требования к своевременной выкладке товара на стеллажах. По оценкам самих ритейлеров, потери от неправильной или несвоевременной выкладки товара могут достигать 5% от общего годового оборота. Учитывая значительный объем оборота крупных сетевых ретейлеров, и заметную текучесть кадров, проблему автоматизации выкладки товара в сетевых магазинах можно считать актуальной. В данной работе представлены результаты разработки автономной робототехнической системы, которая может обеспечить бесперебойный контроль заполнения стеллажей и своевременную выкладку товара. По результатам опроса представителей крупных торговых сетей определены требования к автономной системе контроля и расстановки товаров в магазине. В частности, определены требования к возможностям интеллектуальной системы управления роботом, особенности конструкции и аппаратной реализации роботов, требования к возможностям системы взаимодействия с сотрудниками и покупателями в магазине и предпочтения к внешнему виду и пользовательскому интерфейсу робота. На основе выявленных требований ритейлеров разработан прототип автономного робота для работы в торговых залах. Основа робота представляет собой транспортный модуль с двумя моторколесами и парой рулевых колес, на котором установлен антропоморфный узел с двумя манипуляторами. Манипуляторы выполнены в виде рук человека и имеют весь набор необходимых степеней свободы. Кроме того, в статье представлена архитектура системы управления автономным роботом. За управление роботом отвечает интеллектуальная система принятия решений и управления, основанной на базе мультиагентной нейрокогнитивной архитектуры, моделирующей процессы, протекающие в головном мозге человека. Конструкция и мехатронная часть робота были протестированы в реальных условиях: в торговых залах розничного магазина в г. Нальчик в присутствии продавцов-консультантов и покупателей. В дальнейшем планируются работы по доработке и обучению интеллектуальной системы принятия решений.

Ритейл, роботы; продавец-консультант; искусственный интеллект; инвентаризация полок; мультиагентные нейрокогнитивные архитектуры.