УДК 004.89
DOI: 10.26102/2310-6018/2025.51.4.029

Обнаружение отклонений в сетевых процессах с применением логистической регрессии

И.А. Высоцкая[1]✉, А.В. Скрыпников[2], О.В. Ланкин[2], А.М. Прилуцкий[2], И.А. Коломыцев[2]

[1]Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина, Воронеж, Российская Федерация
[2]Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация

Резюме. При рассмотрении вопросов, связанных с безопасностью компьютерных сетей, особое внимание стоит уделить задачам выявления признаков недетектируемых атак, которые могут оставаться незамеченными стандартными средствами обнаружения и представлять серьезную угрозу для информационных ресурсов организации. Методы машинного обучения приобрели ключевое значение в сфере кибербезопасности, несмотря на существующие трудности их внедрения. Использование современных методов машинного обучения способствует своевременному обнаружению новых видов угроз, повышению эффективности системы защиты и снижению риска возникновения критических инцидентов. Одним из методов машинного обучения является логистическая регрессии, использование которой в рамках системы мониторинга позволяет автоматизировать процессы анализа больших объемов данных, что особенно важно в условиях современных высокоскоростных сетей и непрерывно развивающихся методов кибератак. Данная работа посвящена использованию метода логистической регрессии для обнаружения аномалий в сетевом трафике. Такой подход позволяет эффективно оценивать и выявлять подозрительные сетевые активности, классифицируя объекты как безопасные или потенциально вредоносные. В работе представлен алгоритм создания модели классификатора на основе логистической регрессии для детектирования сетевых аномалий. Обсуждаются вопросы выбора подходящих метрик для оценки модели, сделаны выводы об использовании данного метода как средства распознавания отклонения в сетевых процессах.

Ключевые слова: логистическая регрессия, классификация, информационная безопасность, анализ разнородной информации, машинное обучение, CRISP-DM.

Для цитирования: Высоцкая И.А., Скрыпников А.В., Ланкин О.В., Прилуцкий А.М., Коломыцев И.А. Обнаружение отклонений в сетевых процессах с применением логистической регрессии. *Моделирование, оптимизация и информационные технологии.* 2025;13(4). URL: https://moitvivt.ru/ru/journal/pdf?id=2069 DOI: 10.26102/2310-6018/2025.51.4.029

Detecting deviations in network processes using logistic regression

I.A. Vysotskaya[1]✉, A.V. Skripnikov[2], O.V. Lankin[2], A.M. Prilutsky[2], I.A. Kolomytsev[2]

[1]Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin, Voronezh, the Russian Federation
[2]Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation

Abstract. When considering issues related to computer network security, special attention should be paid to the tasks of identifying signs of undetectable attacks that may remain unnoticed by standard detection tools and pose a serious threat to the organization's information resources. Machine learning methods have acquired key importance in the field of cybersecurity, despite the existing difficulties in their implementation. The use of modern machine learning methods contributes to the timely detection

of new types of threats, increasing the effectiveness of the protection system and reducing the risk of critical incidents. One of the machine learning methods is logistic regression, the use of which within the monitoring system allows you to automate the processes of analyzing large amounts of data, which is especially important in the context of modern high-speed networks and continuously evolving cyberattack methods. This paper is devoted to the use of the logistic regression method to detect anomalies in network traffic. This approach allows you to effectively evaluate and identify suspicious network activities, classifying objects as safe or potentially malicious. The paper presents an algorithm for creating a classifier model based on logistic regression for detecting network anomalies. The issues of choosing suitable metrics for model evaluation are discussed, and conclusions are made about the use of this method as a means of recognizing deviations in network processes.

Keywords: logistic regression, classification, information security, analysis of heterogeneous information, machine learning, CRISP-DM.

For citation: Vysotskaya I.A., Skripnikov A.V., Lankin O.V., Prilutsky A.M., Kolomytsev I.A. Detecting deviations in network processes using logistic regression. *Modeling, Optimization and Information Technology*. 2025;13(4). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=2069 DOI: 10.26102/2310-6018/2025.51.4.029

Введение

Различные виды угроз информационной безопасности могут нанести непоправимый ущерб информационным системам организации, ее репутации и принести серьезные экономические проблемы [1]. Для эффективной идентификации и классификации киберугроз в компьютерных сетях важно учитывать значительное количество факторов, включая пути следования пакетов, задержку передачи данных, потерю пакетов и динамические характеристики трафика, отличающиеся от стабильных состояний. Увеличение объема обрабатываемой аналитической информации и возникновение новых типов атак требуют постоянного улучшения технологий и методик выявления рисков информационной безопасности и повышения надежности защиты каналов связи.

При проектировании системы кибербезопасности предприятия чаще всего используют различные стандартные технические средства защиты информации в совокупности с организационными мерами. Однако злоумышленники находят новые способы нанести критический урон информационным системам и используют ранее неизвестные виды атак. Традиционные методы, такие как сигнатурное обнаружение, правила определения инцидентов часто не справляются с новыми, эволюционирующими видами угроз, особенно с недетектируемыми атаками, которые маскируются под обычный трафик или используют сложные техники обхода систем защиты. Применение современных методов машинного обучения, классификации и кластеризации данных дает возможность структурировать и анализировать большие объемы информации, находить скрытые взаимосвязи, что в итоге позволяет идентифицировать недетектируемые угрозы информационной безопасности [2].

Материалы и методы

Авторы работы [3] утверждают, что ранее использовавшиеся системы безопасности уже неэффективны, поскольку киберпреступники достаточно умны, чтобы обходить традиционные системы защиты. Методы машинного обучения стали играть жизненно важную роль во многих вопросах кибербезопасности, однако имеют свои сложности применения.

В работе [4] рассматриваются различные методы обнаружения сетевых атак и приведена обобщенная классификационная схема. В частности, авторы упоминают о

методах машинного обучения для обнаружения аномалий и злоупотреблений. Отметим, что к их числу относят метод опорных векторов, деревья решений и их ансамбли, методы кластеризации и классификации, нейронные сети. Подробнее остановимся на методах классификации.

Отметим, что линейные модели активно применяются при решении задач классификации. Остановимся подробнее на бинарной классификации, для которой предсказанное значение определяется следующим образом:

$$y = w[0] \cdot x[0] + w[1] \cdot x[1] + \cdots + w[p] \cdot x[p] + b > 0, \quad (1)$$

где $x[0], \ldots x[p]$ – обозначают признаки для отдельной точки данных, *w* и *b* – параметры модели, оцениваемые в ходе обучения, *y* – прогноз, выдаваемый моделью.

В отличие от модели линейной регрессии [5], возвращающей простую взвешенную сумму входных признаков, формула (1) имеет пороговое условие, согласно которому прогнозируемое значение сравнивается с нулем. Когда рассчитанная величина оказывается ниже порога (нуля), модель относит объект к классу с меткой «–1»; в противном случае присваивается метка класса «+1». Такое правило принятия решения характерно для всех линейных классификаторов.

Выходная переменная *y* в линейных моделях регрессии представляет собой линейную комбинацию признаков, и представляет собой прямую линию, плоскость либо гиперплоскость в многомерном пространстве. Границы разделения классов в линейных классификационных моделях также определяются линейными функциями. Среди наиболее популярных линейных алгоритмов классификации выделяются логистическая регрессия и метод опорных векторов [6].

Логистическая регрессия – это метод классификации в машинном обучении, который используется для прогнозирования вероятности принадлежности к некоторому классу, и выдает ответ в виде числа в промежутке от 0 до 1. Стоит отметить, что логистическая регрессия отличается от классической регрессии тем, что она не оценивает конкретные численные значения зависимой переменной. Вместо этого она определяет вероятность принадлежности конкретного наблюдения к определенному классу.

Модель логистической регрессии основана на логистической функции (сигмоиде), которая преобразует линейную комбинацию признаков в вероятность значения от 0 до 1:

$$P(y) = \frac{1}{1+e^{-(w[0]+w[1]x[1]+\cdots+w[n]x[n])}},$$

где $X = (x[0], \ldots, x[n])$ – признаки, а $w[0], w[1], \ldots, w[n]$ – параметры модели.

Коэффициенты $w[i],\ i = \overline{1,n}$ показывают влияние соответствующего признака на вероятность принадлежности к классу. Например, положительный коэффициент означает, что увеличение признака увеличивает вероятность класса с меткой «+1». Параметры модели находят методом максимизации правдоподобия [7].

Обнаружение аномалий в сетевом трафике с помощью логистической регрессии – это подход, при котором модель используется для оценки вероятности того, что конкретный сетевой объект или событие является нормальным или аномальным. Этот метод хорошо подходит для бинарной классификации и прост в интерпретации результатов, что делает его эффективным инструментом для анализа больших объемов сетевого трафика.

Для использования логистической регрессии первоначально необходимо собрать данные о событиях безопасности и создать базу данных. Отметим, что в данном случае задача классификации будет несбалансированной, так как для одного класса

(аномального поведения системы) в выборке существенно меньше примеров, чем для другого.

С помощью логистической регрессии можно выделить различные классы в сетевом трафике на основе различных характеристик, таких как объем переданных данных за сессию, продолжительность соединения, частота запросов, используемые протоколы, IP-адреса источника и назначения. Таким образом возможно определить, является ли конкретное событие (например, соединение, пакет или поток данных) нормальным или аномальным.

Стоит определить ключевые характеристики (признаки), которые будут использоваться для поиска аномалий. Это могут быть такие параметры, например, как IP-адреса. Отметим, что для работы с IP-адресами, их необходимо преобразовать в числовой формат (например, с помощью преобразования в 32-битное целое число).

Любые методы классификации чувствительны к исходным данным, поэтому при анализе стоит обратить внимание на обработку исходных данных. Для получения качественных результатов стоит использовать стандартизацию данных и обработку пропущенных значений. Отметим, что высокоуровневый язык программирования Python обладает специализированными библиотеками и методами для извлечения и подготовки данных.

Обучение модели логистической регрессии может происходить на данных с метками и без. В первом случае подразумевается, что база эталонных данных имеет записи с метками о стационарном поведении и аномальном поведении системы. Иначе, модель обучается на эталонном поведении системы, а все отклонения от предсказанных кластеров считаются аномалией.

После обучения модель выдает вероятность принадлежности события к классу стационарного поведения системы. Значение вероятности, близкое к 1 – состояние системы скорее стационарное, а близкое к 0 – аномальное.

Для использования логистической регрессии в процессе детектирования аномалий устанавливается порог вероятности (например, 0.5 или более строгое значение). Если вероятность ниже порога – событие считается потенциальной аномалией. В процессе использования модели на практике специалист по информационной безопасности может варьировать порогом вероятности, для каждой конкретной исследуемой системы и ее особенностей.

Одной из существенных проблем обучения подобных классификаторов является выбор корректных метрик для оценки качества модели, так как алгоритмы, минимизирующие количество ошибок, могут вырождаться в классификатор, который всегда предсказывает мажоритарный класс.

Результаты

Опишем алгоритм создания модели классификатора на основе логистической регрессии для детектирования сетевых аномалий (Рисунок 1).

В основу положим стандарт CRISP-DM (Cross-Industry Standard Process for Data Mining) [8], который был создан в 1999 году, до сих пор остается актуальным и имеет широкое применение, так как является межотраслевым и не затрагивает особенности отдельных организаций.

На первом этапе – «Постановка задачи», необходимо сформулировать проблему и выбрать целевой параметр, который необходимо улучшить. По этим данным подбирается метрика машинного обучения, с помощью которой в итоге оценивается модель.

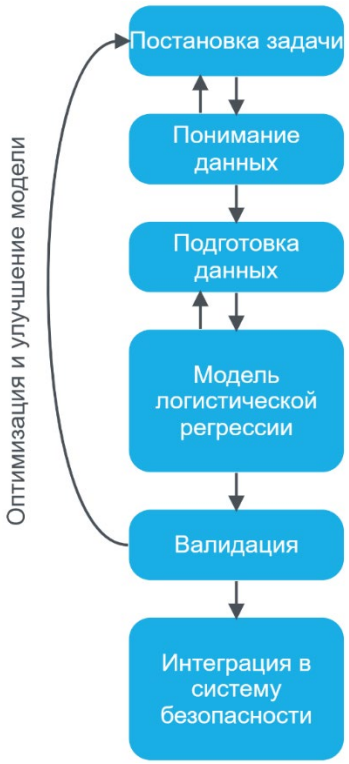

Рисунок 1 – Алгоритм создания модели классификатора на основе логистической регрессии для детектирования сетевых аномалий
Figure 1 – Algorithm for creating a classifier model based on logistic regression for detecting network anomalies

На этапе «Понимание данных» определяются сведения, которые необходимы для решения задачи, их доступность и качество, а также наличие разметки. Если имеющиеся данные не соответствуют поставленной задаче, стоит вернуться на предыдущий этап, для корректировки цели. Опишем каждый тип данных и их влияние на обнаружении аномалий.

Объем данных – это количество байт, переданных за сессию или за определенный промежуток времени. В нормальных условиях наблюдается умеренный объем (например, около 500 байт). В аномальных случаях – значительно выше, что может указывать на атаки типа DDoS или массовое сканирование.

Длительность соединения – время, в течение которого соединение было активно, измеряется в секундах. Аномалии характеризуются длинными соединениями (300-400 секунд), что может указывать на злоумышленника или бота.

Количество запросов – общее число запросов или пакетов за сессию. Высокая частота запросов может указывать на автоматизированные атаки или сканирование.

Уровень ошибок – доля ошибок или повторных попыток в сессии. Низким значением считают около 1 % ошибок; при аномалиях наблюдается высокий уровень ошибок (20–30 %), что может свидетельствовать о неправильных командах, попытках взлома или сбоях. В совокупности эти признаки позволяют модели отличать обычное поведение сети от подозрительного.

Этап «Подготовка данных» предполагает выполнение множества различных операций. Работа с данными начинается с проверки их качества и обработки. Далее необходимо преобразовать переменные в формат, подходящий для модели. Так, для логистической регрессии стоит использовать численные или категориальные переменные, учитывая специфику задачи. Перед включением каждого признака в модель

необходимо проверить его значимость, таким образом можно избежать излишней детализации и упростить задачу. Отметим, что не информативные признаки могут не только не обладать важной информацией, но и влиять на качество модели, снижать ее работоспособность.

Этап «Модель логистической регрессии» включает в себя обучение модели и подбор параметров. Если модель не показывает требуемого качества, то стоит вернуться к этапу «Подготовка данных», и выбрать другие признаки или пересмотреть их значимость. Этап моделирования завершается сравнением нескольких моделей, после чего отдают предпочтение той, которая показала высокое качество.

Основная цель «Валидации» заключается в проверке наличия скрытых аспектов модели перед ее внедрением, которые могли остаться незамеченными ранее. В частности, полученная модель может плохо справляться с целевыми задачами, хотя на метрике машинного обучения показывать высокие результаты. Если модель отклонена, мы возвращаемся на этап «Постановка задачи» и «Понимание данных».

Последним этапом является «Интеграция в систему безопасности» – внедрение в систему безопасности, с учетом имеющихся ресурсов защищаемого объекта. Развертывается производственная версия модели, интегрированная с системой мониторинга и реагирования на инциденты. В процессе эксплуатации проводится регулярная проверка точности и настройка пороговых значений. Важно отметить, что со временем модель может утратить свою эффективность вследствие изменения стационарного поведения системы, поэтому рекомендуется периодически обновлять модель, используя актуальные наборы данных.

Предложенный алгоритм обладает уникальной комбинацией универсальности подхода, эффективности выявления скрытых угроз и гибкости адаптации под разнообразные условия функционирования информационных систем. Большинство существующих методов часто фокусируются лишь на этапе выбора и обучения модели.

Однако предложенный алгоритм предусматривает полный цикл работ, при этом логистическая регрессия отлично интегрируется в концепцию CRISP-DM, гарантируя оптимальное соотношение между качеством результата, быстротой исполнения и экономическими затратами.

Модель логистической регрессии для обнаружения сетевых аномалий, была реализована на языке Python. В качестве входных данных использовалось около 500 записей с поведением защищаемой системы, включающие в себя объем данных, длительность соединения, количество запросов, уровень ошибок. После обучения модель выдает вероятность для каждого нового соединения. Если вероятность ниже установленного порога, то это событие помечается как потенциальная атака или вредоносная активность.

Обсуждение

Рассмотрим результаты работы модели логистической регрессии по различным метрикам (Таблица 1).

Таблица 1 – Оценка модели логистической регрессии
Table 1 – Estimation of the logistic regression model

Класс	Precision	Recall	F1-score	Support
Норма	0,85	0,90	0,87	69
Аномалия	0,74	0,65	0,69	21

Support (Поддержка) показывает количество примеров каждого класса в тестовом наборе. Можно сделать вывод, что большее число нормальных примеров привело к лучшим показателям точности и полноты для этого класса. Задача распознавания не детектируемых угроз, с точки зрения машинного обучения, является задачей с дисбалансом классов. Целью является поиск объектов, которые не похожи на большинство объектов из обучающей выборки. При этом примеров аномалий либо нет вовсе, либо мало.

Так как мы видим дисбаланс классов, то выбор в качестве метрики Accuracy (Точность) приведет к неправильной оценке модели. В таком случае наиболее подходящими метриками являются Precision (Точность), Recall (Полнота) и F1-score.

Precision (Точность) показала, что из всех точек, классифицированных как нормальные, действительно нормальными оказались 85 %, а для аномалии – 74 %.

Recall (Полнота) – среди всех примеров со стационарным поведением системы 90 % были найдены и классифицированы правильно. Однако только 65 % аномалий были обнаружены моделью.

Значение 0,8 для F1-score показывает хороший компромисс между точностью и полнотой, однако низкое значение 0,69 указывает на сложность точного распознавания аномалий.

Стоит отметить, что для задач классификации с дисбалансом классов, важно в качестве результатов получать вероятности, а не метки классов (пользоваться методом predict_proba вместо predict, для языка программирования Python) и подбирать порог классификации, исходя из выбранных метрик.

Среди ограничений и особенностей использования логистической регрессии можно отметить, что для сложных нелинейных закономерностей могут потребоваться более усовершенствованные модели. Для повышения точности результатов возможно комбинировать логистическую регрессию с другими методами обнаружения аномалий. С развитием машинного обучения и обработки больших данных классическая логистическая регрессия расширяется за счет использования регуляризации (LASSO, Ridge), внедрение нелинейных преобразований признаков, а также интеграции с ансамблевыми моделями.

Полученные результаты, основанные на использовании модели логистической регрессии, могут стать фундаментом для разработки автоматизированной системы принятия решений в области информационной безопасности. Основываясь на результатах анализа сетевого трафика в реальном времени, такая система сможет оценивать вероятность недетектируемой атаки. При выявлении события, которое выходит за рамки стационарного поведения анализируемой системы, и классифицируемое как потенциально вредоносное, система безопасности может блокировать его, уведомлять специалистов или проводить дополнительные проверки. Такой подход значительно повысит устойчивость системы безопасности и ускорит время обработки инцидентов. Кроме того, автоматизация процесса принятия решений обеспечит системный и последовательный подход к защите информационных ресурсов.

Заключение

В последние годы особое внимание уделяется машинному обучению для автоматизации процесса обнаружения угроз. Логистическая регрессия традиционно применяется для задач бинарной классификации, ее можно эффективно использовать и для обнаружения сетевых аномалий, особенно в сочетании с правильной подготовкой данных и признаков. В сравнении с более сложными моделями (например, случайным лесом [9] или нейронными сетями [10]) логистическая регрессия показывает

сопоставимую точность при меньших требованиях к вычислительным ресурсам и большей прозрачности решений. Так, например, можно оценить влияние каждого из признаков на вероятность возникновения аномального поведения исследуемой системы. Однако отметим и сложности, которые могут возникнуть из-за дисбаланса классов, поэтому для повышения точности рекомендуется комбинировать логистическую регрессию с другими методами анализа и обработки данных, а также выбирать в качестве метрик Precision, Recall и F1-score.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Ершова Е.Е. Информационная безопасность как элемент экономической безопасности. *Управление образованием: теория и практика*. 2022;12(6):225–230. https://doi.org/10.25726/v8343-7232-2832-p
   Ershova E.E. Information Security as an Element of Economic Security. *Education Management Review*. 2022;12(6):225–230. (In Russ.). https://doi.org/10.25726/v8343-7232-2832-p
2. Высоцкая И.А. Обнаружения сетевых атак с использованием методов статистического анализа. В сборнике: *Информатика: проблемы, методы, технологии: Материалы XXI Международной научно-методической конференции, 11–12 февраля 2021 года, Воронеж, Россия.* Воронеж: Вэлборн; 2021. С. 240–243.
3. Shaukat K., Luo S., Varadharajan V., Hameed I.A., Xu M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*. 2020;8:222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951
4. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН*. 2016;(2):207–244. https://doi.org/10.15622/sp.45.13
   Branitskiy A., Kotenko I. Analysis and Classification of Methods for Network Attack Detection. *SPIIRAS Proceedings.* 2016;(2):207–244. (In Russ.). https://doi.org/10.15622/sp.45.13
5. Бахтин И.В. Модель линейной регрессии с использованием библиотеки Scikit-Learn. *Инновации. Наука. Образовани*е. 2021;27:939–951.
6. Баев Н.О. Использование метода опорных векторов в задачах классификации. *Международный журнал информационных технологий и энергоэффективности.* 2017;2(2):17–21.
   Baev N.O. Using the Method of Support Vectors in Classification Tasks. *Mezhdunarodnyi zhurnal informatsionnykh tekhnologii i energoeffektivnosti.* 2017;2(2):17–21. (In Russ.).
7. Астапов Р.Л., Мухамадеева Р.М. Автоматизация подбора параметров машинного обучения и обучение модели машинного обучения. *Актуальные научные исследования в современном мире*. 2021;(5–2):34–37.
   Astapov R.L., Mukhamadeeva R.M. Selection's Automatization of Machine Learning Parameters and Training a Machine Learning Model. *Aktual'nye nauchnye issledovaniya v sovremennom mire*. 2021;(5–2):34–37. (In Russ.).
8. Matthies B. CRISP-DM: das Vorgehensmodell für Data Mining. *WiSt. Wirtschaftswissenschaftliches Studium.* 2022;51(5):42–44. (In German). https://doi.org/10.15358/0340-1650-2022-5-42
9. Марахимов А.Р., Кудайбергенов Ж.К., Худайбергенов К.К., Охундадаев У.Р. Многомерный двоичный классификатор дерева решений на основе неглубокой нейронной сети. *Научно-технический вестник информационных технологий,*

механики и оптики. 2022;22(4):725–733. (На англ.). https://doi.org/10.17586/2226-1494-2022-22-4-725-733
Marakhimov A.R., Kudaybergenov J.K., Khudaybergenov K.K., Ohundadaev U.R. A Multivariate Binary Decision Tree Classifier Based on Shallow Neural Network. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* 2022;22(4):725–733. https://doi.org/10.17586/2226-1494-2022-22-4-725-733

10. Скрыпников А.В., Берестовой А.А., Никульчева О.С., Зиновьева В.В. Оптимизация информационно-телекоммуникационных систем с использованием нейронных сетей: повышение эффективности и безопасности. *Вестник Воронежского института ФСИН России.* 2024;(4):135–139.
Skrypnikov A.V., Berestovoy A.A., Nikulcheva O.S., Zinovieva V.V. Optimization of Information and Telecommunication Systems Using Neural Networks: Improving Efficiency and Safety. *Vestnik Voronezhskogo instituta FSIN Rossii*. 2024;(4):135–139. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Высоцкая Ирина Алевтиновна, доктор технических наук, доцент кафедры математики, Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина, Воронеж, Российская Федерация.
e-mail: i.a.trishina@gmail.ru
ORCID: 0000-0001-6521-9570

Irina A. Vysotskaya, Doctor of Engineering Sciences, Associate Professor at the Department of Mathematics, Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin, Voronezh, the Russian Federation.

Скрыпников Алексей Васильевич, доктор технических наук, профессор, заведующий кафедрой информационной безопасности, Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация.
e-mail: skrypnikovvsafe@mail.ru
ORCID: 0000-0003-1073-9151

Alexey V. Skrypnikov, Doctor of Engineering Sciences, Professor, Head of the Department of Information Security, Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation.

Ланкин Олег Викторович, доктор технических наук, доцент, профессор кафедры информационной безопасности, Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация.
e-mail: oleg_lankin@mail.ru

Oleg V. Lankin, Doctor of Engineering Sciences, Docent, Professor at the Department of Information Security, Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation.

Прилуцкий Александр Михайлович, кандидат технических наук, доцент, доцент кафедры информационной безопасности, Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация.
e-mail: pam71@mail.ru

Alexander M. Prilutsky, Candidate of Engineering Docent, Associate Professor at the Department of Information Security, Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation.

Коломыцев Илья Андреевич, аспирант, Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация.
e-mail: ilyakolomytsev@yandex.ru

Ilya A. Kolomytsev, Postgraduate, Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation.

Статья поступила в редакцию 05.09.2025; одобрена после рецензирования 15.10.2025; принята к публикации 27.10.2025.

The article was submitted 05.09.2025; approved after reviewing 15.10.2025; accepted for publication 27.10.2025.