Научная статья
УДК 004.056.53
https://doi.org/10.24143/2072-9502-2025-4-33-42
EDN FJTNNB

Алгоритм обнаружения аномального поведения пользователей автоматизированных систем на основе методов машинного обучения

Евгений Евгеньевич Трунов

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко,
Краснодар, Россия, ittehnology2018@gmail.com

Аннотация. В настоящее время актуальным направлением исследований является разработка современных решений для анализа паттернов поведения пользователей, которые в профессиональной среде известны как системы аналитики поведения пользователей и сущностей. Предлагается рассмотреть возможность построения таких систем с использованием методов машинного обучения. Это обусловлено увеличением источников и объема данных о пользователе, в результате чего ручной анализ трудозатратен, а классические методы на основе статистики или правил не всегда обеспечивают требуемое качество детекции аномалий. Целью работы является построение эффективного алгоритма машинного обучения для задачи обнаружения аномалий в данных. Предложен алгоритм обнаружения аномального поведения пользователей автоматизированных систем, а также оптимизационный алгоритм на основе искусственной иммунной системы для выбора наилучших гиперпараметров алгоритма. Алгоритм обнаружения аномалий основан на классификации поведения пользователей в системе на основе их действий с использованием модели генеративно-состязательной сети. Предлагаемый алгоритм позволяет генерировать дополнительные выборки с распределением генеральной совокупности в целях сокращения времени внедрения и классифицировать пользователей на основе сформированных паттернов нормального поведения. Отличительная особенность алгоритма заключается в его способности адаптироваться к реальной системе, обучаясь на пользовательских данных и сохраняя при этом заданную точность классификации благодаря автоматическому подбору оптимальных гиперпараметров. Научная новизна предлагаемого алгоритма заключается в добавлении процедуры кластеризации в процесс аннотирования данных перед обучением модели машинного обучения, а также адаптации генеративно-состязательной сети для задачи обнаружения аномалий в данных путем изменения алгоритма обучения. Предлагаемый подход позволит с высокой точностью выявлять отклонения от нормального поведения пользователей в автоматизированном режиме и приближенно к реальному времени, что сократит время обработки событий информационной безопасности.

Ключевые слова: машинное обучение, обнаружение аномалий, поведенческий анализ, безопасность информации

Для цитирования: *Трунов Е. Е.* Алгоритм обнаружения аномального поведения пользователей автоматизированных систем на основе методов машинного обучения // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2025. № 4. С. 33–42. https://doi.org/10.24143/2072-9502-2025-4-33-42. EDN FJTNNB.

Original article

Algorithm for detecting anomalous behavior of users of automated systems based on machine learning methods

Evgeny E. Trunov

Krasnodar Higher Military awarded by the Orders of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S. M. Shtemenko,
Krasnodar, Russia, ittehnology2018@gmail.com

Abstract. Currently, a relevant area of research is the development of modern systems for analyzing user behavior and entities, which are professionally known as user behavior and entity behavior analytics systems. It is proposed to consider the possibility of building such systems using machine learning methods. This is due to an increase in the sources and volume of user data, as a result of which manual analysis is labor-intensive, and classical methods based on statistics or rules do not always provide the required quality. The aim of the work is to build an effective machine learning algorithm for the task of detecting anomalies in data. An algorithm for detecting abnormal behavior of users of automated systems is proposed, as well as an optimization algorithm based on the artificial immune system for selecting the best hyperparameters of the algorithm. The anomaly detection algorithm is based on the classification of user behavior in the system based on their actions using the generative-adversarial network model. The proposed algorithm makes it possible to generate additional samples with a general probability distribution in order to reduce the implementation time and classify users based on the formed patterns of normal behavior. A distinctive feature of the algorithm is its ability to adapt to a real system, learning from user data while maintaining a given classification accuracy due to the automatic selection of optimal hyperparameters. The scientific novelty of the proposed algorithm consists in adding a clustering procedure to the process of data annotation before training a machine learning model, as well as adapting a generative-adversarial network for the task of detecting anomalies in data by changing the learning algorithm. The proposed approach will make it possible to detect deviations from normal user behavior with high accuracy in automated mode and close to real time, which will reduce the processing time for information security events.

Keywords: machine learning, anomaly detection, behavioral analysis, information security

For citation: Trunov E. E. Algorithm for detecting anomalous behavior of users of automated systems based on machine learning methods. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2025;4:33-42. (In Russ.). https://doi.org/10.24143/2072-9502-2025-4-33-42. EDN FJTNNB.

Введение

В современных условиях, когда объемы данных продолжают расти с экспоненциальной скоростью, а количество пользователей информационных систем увеличивается, проблема контроля пользователей и их информационных потоков становится более актуальной, чем когда-либо. В качестве систем, направленных на решение поставленной проблемы, выступает класс программных решений поведенческой аналитики пользователей, в профессиональной сфере известных как User and Entity Behavior Analytics (UEBA), – системы анализа поведения пользователей и сущностей. Решения данного класса являются ключевым инструментом для выявления и предотвращения потенциальных угроз в автоматизированных системах за счет обнаружения отклонений в действиях пользователей. Вопрос обнаружения аномального поведения пользователей на основе анализа действий в системе актуален уже не одно десятилетие, меняя вектор своего развития, т. к. постоянно появляются новые технологии и меняются существующие. Так, одним из активно развивающихся направлений является использование в UEBA-системах алгоритмов интеллектуальной обработки данных и машинного обучения [1].

Существующие работы по теме исследования предлагают различные подходы к реализации выявления аномалий в действиях пользователя, но при этом имеют ряд существенных недостатков. Так, в отдельных работах [2–4] предлагается использовать статистические и линейные алгоритмы, что является эффективным только в случаях, когда анализ проводится на небольшой выборке и ограниченным набором признакового пространства. В то же время современные условия функционирования автоматизированных систем диктуют обратное: множество разнородных источников данных и большое количество событий, которые требуется анализировать в совокупности. Другая часть работ [5–8] учитывает особенности функционирования автоматизированных систем, и авторы предлагают использовать модели машинного обучения для обнаружения аномалий, но при этом по-прежнему анализ производится только на ограниченном признаковом пространстве и рассматривает поведение пользователя само по себе, без учета сущностей работы системы.

Алгоритм обнаружения аномального поведения пользователей

На основе проведенного анализа существующих подходов в исследовании предлагается использовать более современную генеративно-состязательную модель машинного обучения (GANs), структурно состоящую из двух нейронных сетей (генератора и дискриминатора).

Важно отметить, что используемый в работе метод генеративно-состязательной сети относится к классу методов глубокого машинного обучения, основанных на нейронных сетях. В отличие от традиционных алгоритмов машинного обучения (например, SVM, Random Forest, Isolation Forest), которые в основном применяются к строго структурированным данным, нейронные сети и, в частности, генеративно-состязательные сети обладают способностью обрабатывать сложные, частично неструктурированные данные, такие как поведенческие признаки пользователей, журналы действий, последовательности событий и др. Это особенно важно в задачах анализа поведения, где высокая

изменчивость и сложная семантика данных ограничивают применение классических подходов. Генеративно-состязательные сети позволяют моделировать латентные закономерности в поведенческих паттернах и выявлять отклонения, выходящие за пределы обученного распределения. Таким образом, использование именно предлагаемого метода, а не более простых моделей обусловлено необходимостью гибкой обработки разнообразных и потенциально неструктурированных поведенческих признаков в рамках автоматизированных систем.

В задачи генератора входит создание новых данных с распределением генеральной совокупности, что позволит сократить время внедрения предлагаемого решения до 1 месяца, в то время как существующие UEBA-системы требуют для сбора данных и обучения от 3 до 6 месяцев непрерывного функционирования. Дискриминаторную модель предлагается использовать в режиме бинарного классификатора, что позволит отделять нормальное поведение пользователя от аномалий. В ходе состязательного обучения генератора и дискриминатора, где генератор будет стремиться создавать максимально правдоподобные примеры поведения пользователя, а дискриминатор находить отличия между исходной и генерируемой совокупностью данных, мы будем стремиться минимизировать ошибки работы дискриминатора. Данный подход отличается от эталонной модели генеративно-состязательных сетей, где минимизируют ошибки генератора исходя из первоначальной задачи этого класса моделей. Также предлагается добавить кластеризацию данных перед обучением генеративно-состязательной сети, это позволит дискриминатору точнее определять аномалии по классу пользователей и заведомо уберет выбросы (пользователей, не похожих на свою группу). Данный способ также отличается от предлагаемых решений UEBA-систем, анализ которых приведен далее, где используются данные из единого пространства пользователей для формирования классов. При таком подходе, в случае наличия в группе легитимного пользователя с повышенными привилегиями, система будет его определять как аномалию по классу, что придется фильтровать вручную. Предлагаемый же подход позволяет автоматизировать данный процесс в целях сокращения времени обнаружения аномальных событий информационной безопасности. Схема работы предлагаемого алгоритма представлена на рис. 1. Обучение модели генеративно-состязательной сети проводилось на выборочной совокупности действий 800 пользователей, собираемых в течение месяца. Признаковое пространство включает несколько основных блоков данных о поведении пользователей:

– пользователь (ID пользователя);

– журнал удаленного доступа (данные о подключении к службе удаленных рабочих столов);

– мониторинг процессов (данные о запускаемых процессах и их количество);

– мониторинг доступа к USB (данные о действиях пользователя с отчуждаемыми машинными носителями информации);

– сетевая активность (данные о количестве полученного и отправленного трафика);

– локальные действия пользователей (биометрические данные пользователя);

– системные метрики (данные о загруженности ресурсов автоматизированной системы);

– журнал аутентификации (данные о процессе аутентификации пользователя);

– изменение файловой системы (действия с файловой системой).

Перед подачей данных для обучения производится их предварительная обработка, включающая кодирование категориальных признаков, нормализацию значений, обработку выбросов и пропущенных значений. Методом One-Hot Encoding каждый категориальный тип данных представляется как отдельный бинарный столбец. Нормализация данных осуществляется логарифмическим преобразованием (натуральный для экспоненциальных значений признаков и десятичный для признаков разного порядка). Применение данного метода нормализации обусловлено широким диапазоном значений и требованием к сохранению информативности каждого признака. Подробное описание формирования признакового пространства для задачи обнаружения аномального поведения пользователей представлено в статье [9], где рассмотрены все основные этапы предварительной обработки и обоснование применяемых методов.

Обучение генеративно-состязательной сети происходит с использованием иммунного алгоритма оптимизации, эффективность которого уже была доказана [10, 11] в сравнении с полным перебором или случайным поиском. Алгоритм параметрической оптимизации гиперпараметров модели машинного обучения на основе алгоритма искусственной иммунной системы реализован в виде программы для ЭВМ [12], блок-схема которой представлена на рис. 2. Блок 3 определяет научную новизну предлагаемого алгоритма, которая заключается в добавлении весового коэффициента значимости в процесс мутации.

Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2025. № 4
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)
Компьютерное обеспечение и вычислительная техника

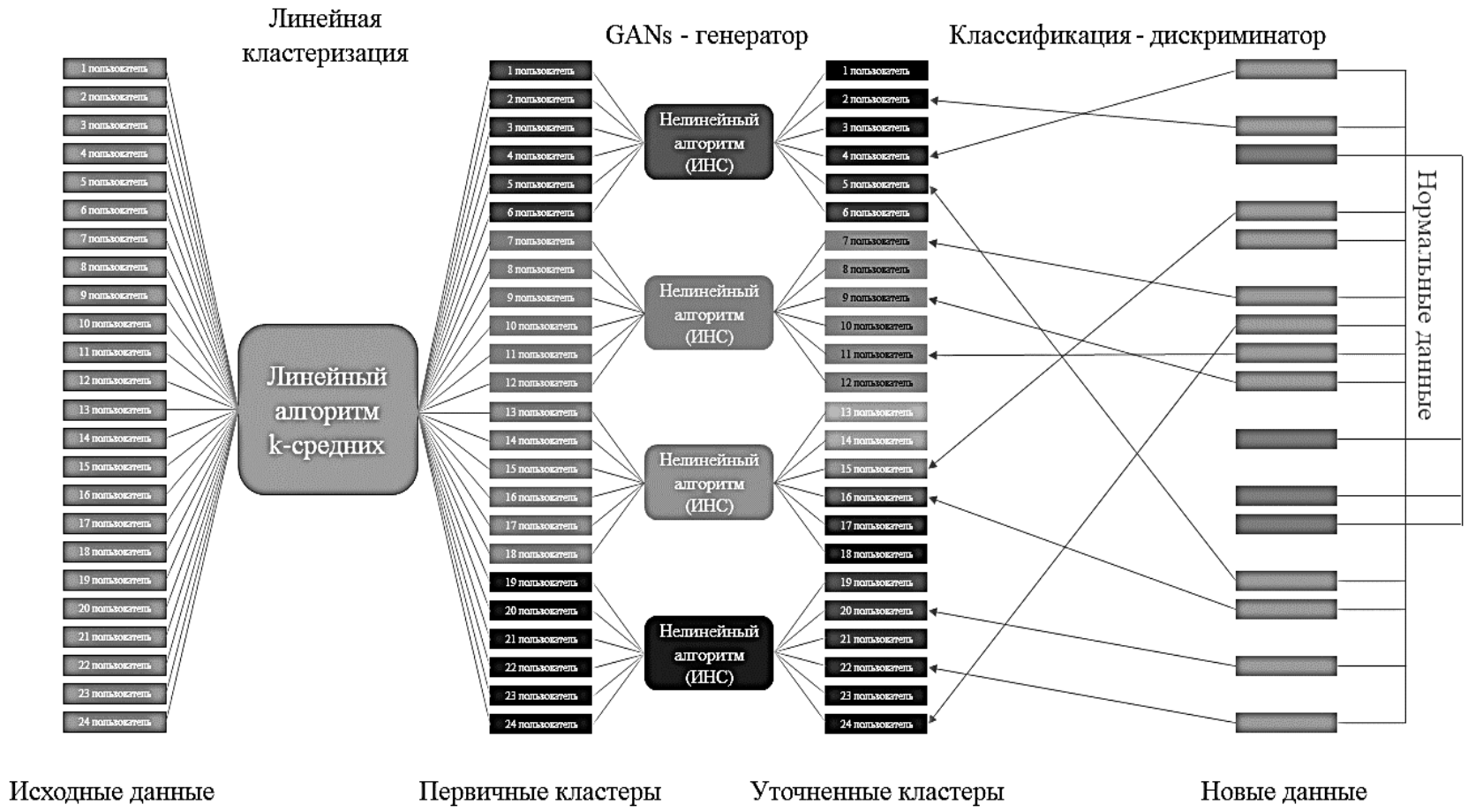
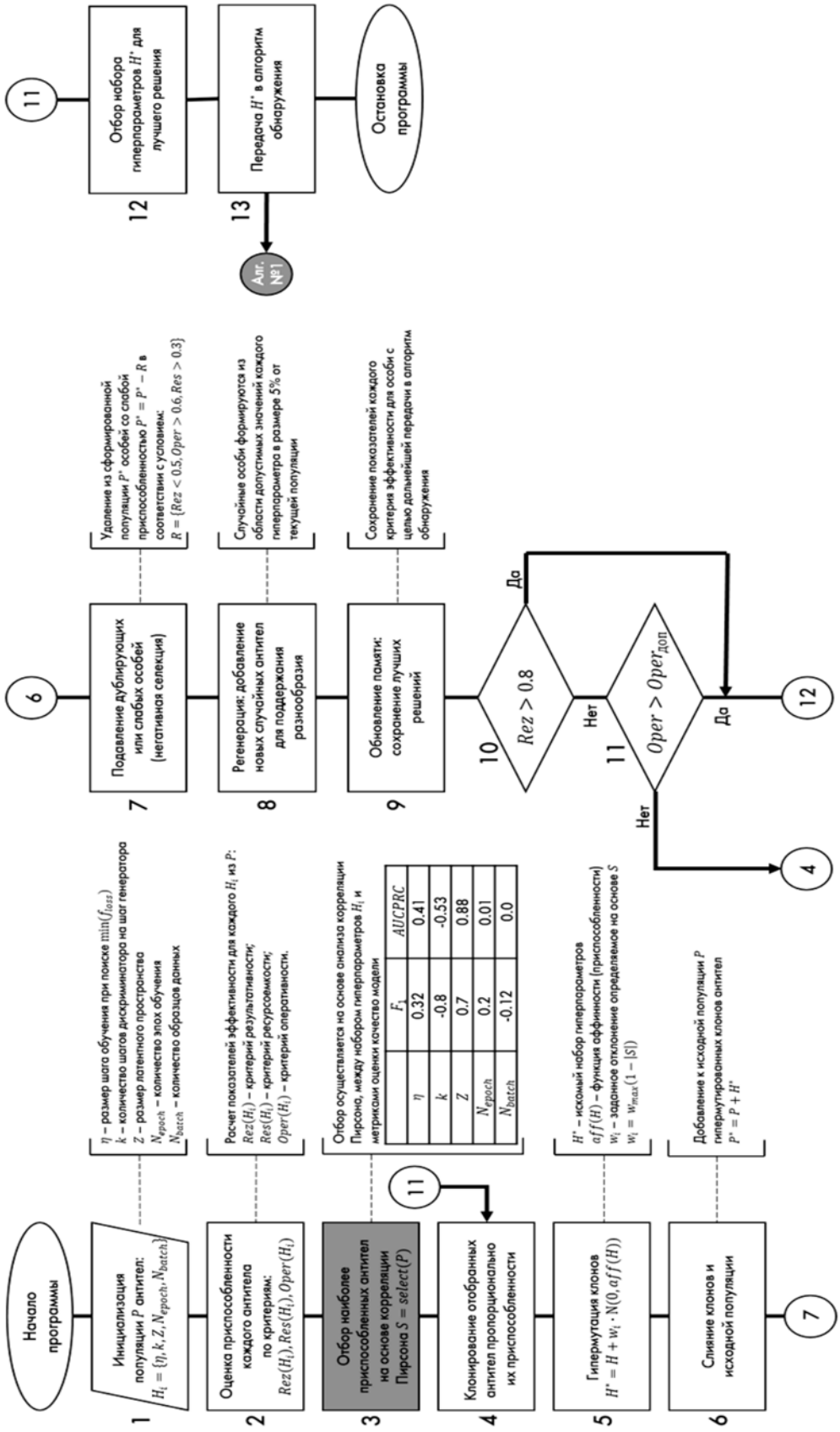


Рис. 1. Схема работы алгоритма обнаружения аномалий в данных

Fig. 1. Scheme of the operation of the data anomaly detection algorithm



	F_1	$AUCPRC$
η	0.32	0.41
k	-0.8	-0.53
Z	0.7	0.88
N_{epoch}	0.2	0.01
N_{batch}	-0.12	0.0

Рис. 2. Блок-схема программы параметрической оптимизации

Fig. 2. Block diagram of the parametric optimization program

Входными данными алгоритма является набор гиперпараметров, к которым применяется иммунный алгоритм параметрической оптимизации. Выходными данными является матрица оптимальных гиперпараметров, которые передаются в предлагаемый алгоритм обнаружения на основе генеративно-состязательной нейронной сети.

Главной задачей процесса оптимизации является подбор наилучшего набора гиперпараметров H^* из области допустимых значений Q, от которых напрямую зависит эффективность работы предлагаемого алгоритма:

$$H^* = \arg\max_H E(H), H \to Q.$$

Целевая функция зависит от трех ключевых параметров: результативности (*Rez*), оперативности (*Oper*) и ресурсоемкости (*Res*). В представленной постановке задача является многокритериальной и заключается в нахождении Парето-оптимальных решений. Результирующее значение эффективности E получается путем мультипликативной свертки параметров и добавлением весовых коэффициентов значимости w_i каждого параметра, значение которых определяется экспертным методом:

$$E = \frac{Rez^{w_1}}{Oper^{w_2} \cdot Res^{w_3}}.$$

В качестве составляющих для расчета результативности предлагаемого алгоритма выступают метрики оценки качества моделей машинного обучения, выбранные в соответствии с национальным стандартом [13], а именно показатель *F*-меры и площади под кривой ROC (roc-auc). Результаты расчета комплексного показателя результативности с использованием стандартной модели иммунного алгоритма, представленные на рис. 3, показывают низкую скорость сходимости показателей при переходе от поколения к поколению.

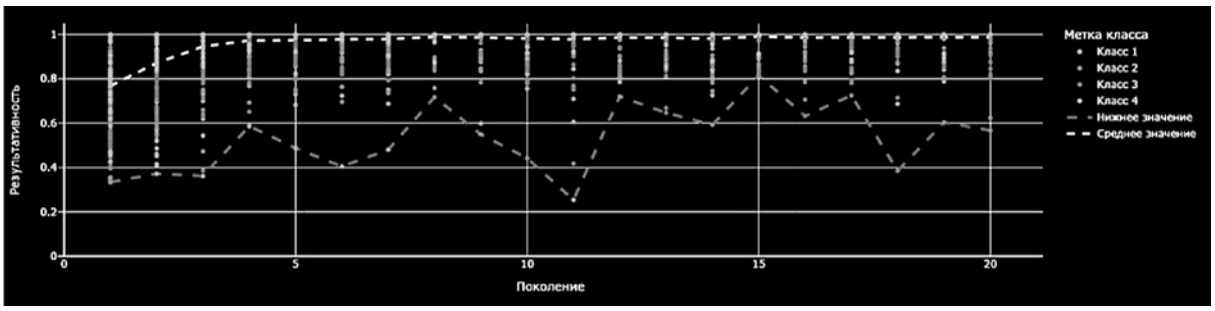


Рис. 3. Распределение показателя результативности по поколениям

Fig. 3. Distribution of the performance indicator by generations

В целях устранения выявленного недостатка предлагается введение весовых коэффициентов w_i значимости гиперпараметров в механизм мутации, данный коэффициент определяется на основе матрицы корреляции Пирсона и имеет прямо пропорциональную зависимость:

$$x_i = x_{i-1} + w_i \cdot N(0, D(aff(x_i))).$$

На каждом поколении формируется множество особей (наборов гиперпараметров) x, которые мутируют с определенным отклонением N. Область допустимых значений отклонения рассчитывается для каждой особи на основе функции аффинности *aff*, которая определяет качество модели по метрикам *F*-меры и roc-auc. Добавленный весовой коэффициент влияет на дисперсию мутации: чем выше вес гиперпараметра, тем меньше он мутирует. Результаты расчета комплексного показателя результативности с учетом весовых коэффициентов значимости представлены на рис. 4.

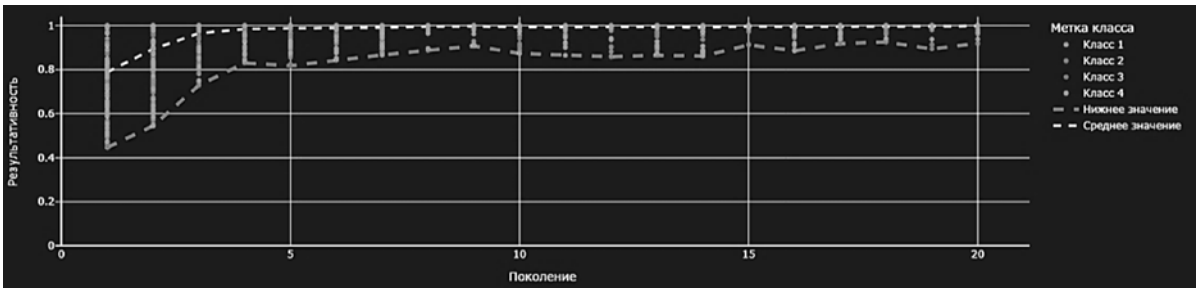


Рис. 4. Распределение показателя результативности по поколениям

Fig. 4. Distribution of the performance indicator by generations

Добавление весового коэффициента в процесс мутации позволяет сохранить значение наиболее значимого гиперпараметра в каждом поколении мутации. По результатам сравнения полученных значений комплексного показателя результативности было выявлено повышение скорости сходимости оптимизационного алгоритма на каждой итерации.

Оценка результативности предлагаемого алгоритма

В ходе исследования был проведен анализ существующих решений UEBA [14–17] и выделены основные алгоритмы, используемые в них. Часть решений использует предобученные модели машинного обучения, которые не отражают действительное положение дел в автоматизированных системах, а следовательно, анализируют лишь шаблонное поведение пользователей, которое заранее заложено в исходных данных для обучения. Другая же часть решений предлагает как статистические алгоритмы анализа, так и применение методов машинного обучения, таких как k-means (алгоритм k-средних), Isolation Forest (модель изоляционного леса), SVM (метод опорных векторов), DBSCAN (алгоритм кластеризации на основе плотности распределения), LOF-mod (алгоритм локальных выбросов).

На основе данных, полученных в ходе анализа, было проведено сравнение предлагаемого алгоритма с уже существующими методами на выборочной совокупности исходных данных. Результаты сравнения (рис. 5) показывают, что наилучшие результаты показали алгоритм локальных выбросов (LOF-mod) и предлагаемый в работе алгоритм генеративно-состязательной сети (GANs).

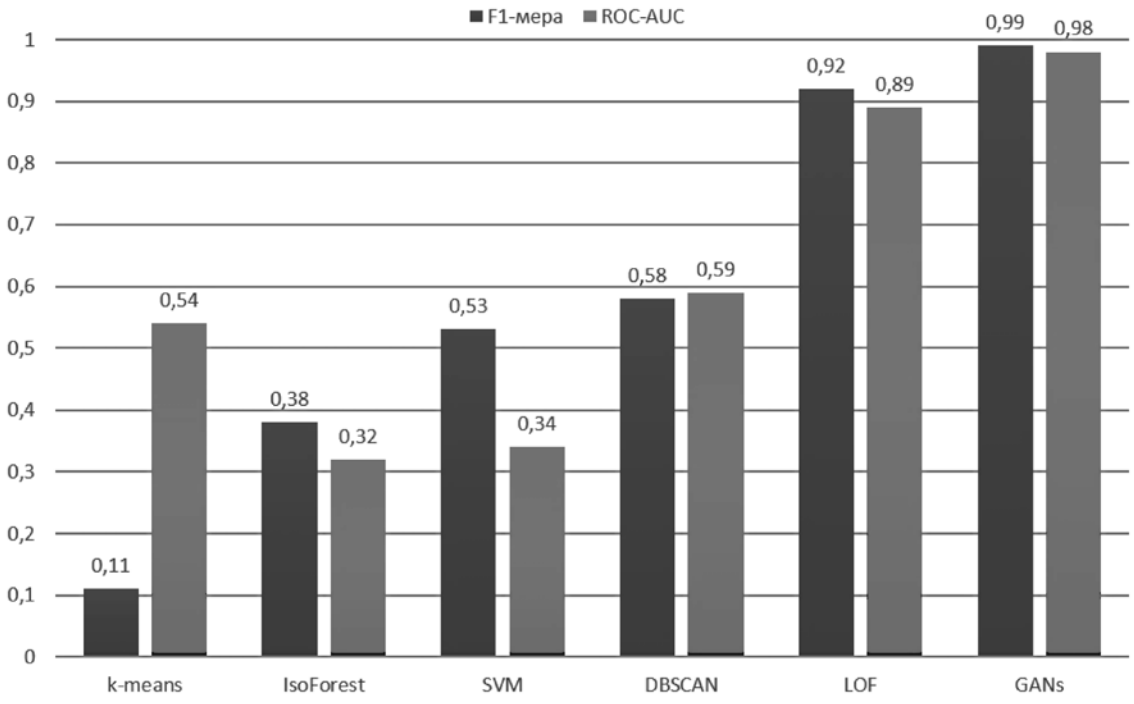


Рис. 5. Сравнительный анализ алгоритмов обнаружения аномалий в данных

Fig. 5. Comparative analysis of data anomaly detection algorithms

Таким образом, прирост в результативности предлагаемого алгоритма в сравнении с LOF-mod составляет 7,6 % по метрике F1-мера и 10 % по метрике ROC-AUC. Несмотря на близкие количественные показатели эффективности вышеупомянутых алгоритмов, предлагаемое в работе решение способно быстрее интегрироваться в систему ввиду отсутствия необходимости сбора большого набора данных.

Матрица ошибок для данной модели демонстрирует ее высокую точность и способность эффективно различать классы: из 10 000 событий модель правильно предсказала 4 815 положительных случаев (True Positives (TP)) и 4 875 отрицательных (True Negatives (TN)), при этом были допущены 125 ложноположительных ошибок (False Positives (FP), когда модель ошибочно отнесла отрицательные события к положительным, и 185 ложноотрицательных ошибок (False Negatives (FN)), когда положительные события были неверно классифицированы как отрицательные (табл.).

Матрица ошибок

Error matrix

Истинный класс	Предсказано положительное	Предсказано отрицательное
Истинно положительное	TP = 4 815	FN = 185
Истинно отрицательное	FP = 125	TN = 4 875

Данные значения соответствуют усредненным значениям метрик модели: F1-мера – 0,9629, ROC-AUC – 0,9761 и PR-AUC – 0,9754, что подтверждает ее точность в идентификации классов и низкий уровень ошибок первого и второго рода.

Распределение событий информационной безопасности в ходе моделирования представлено на рис. 6.

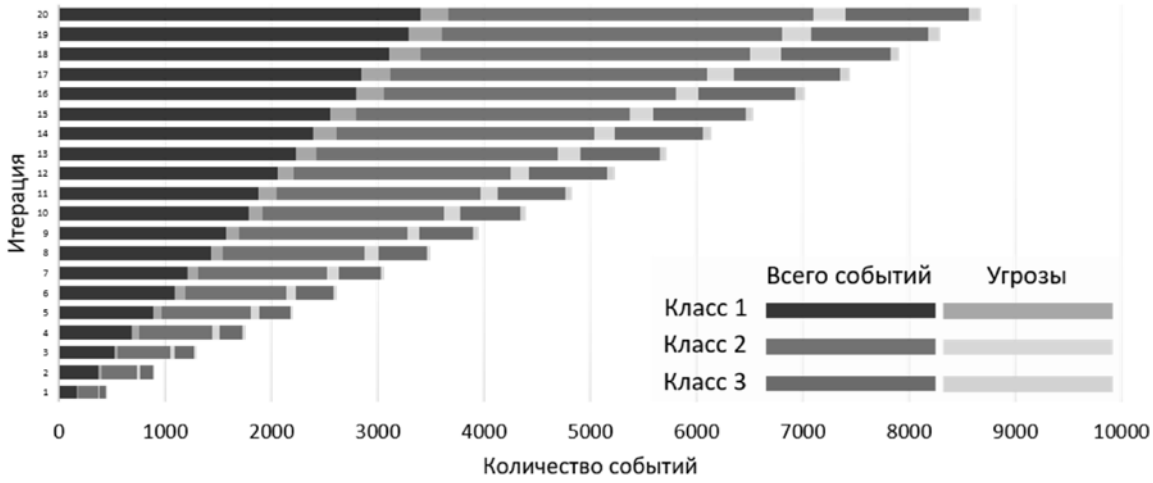


Рис. 6. Распределение событий информационной безопасности

Fig. 6. Distribution of information security events

Гистограмма показывает накопление событий по 3 классам на каждом шаге процесса моделирования, а также долю угроз от общего числа событий, которые имитируются в модели. Каждый класс событий отражает группу пользователей, которые анализируются на аномальное поведение. Классы событий определяются путем предварительной кластеризации с использованием алгоритма k-средних. Под угрозами в данном случае понимаются аномальные события, которые отражают поведение внутреннего злоумышленника. На 20-й итерации происходит накопление минимального числа событий моделирования (10 000 событий), из которых 8 725 событий подвергаются анализу, а 1 275 попадают в блок сброса, т. к. не отнесены ни к одному классу событий. Минимальное число событий для моделирования рассчитывалось путем сравнения эмпирического и теоретического распределения с использованием критерия Пирсона.

Моделирование процесса обнаружения аномального поведения пользователей в автоматизированной системе производилось в среде имитационного моделирования CPNTools с использованием встроенного языка программирования CPN-ML. В модели учтены основные характеристики рассматриваемого объекта, такие как структура, распределение показателей функционирования и временные характеристики.

Заключение

Предлагаемый в работе алгоритм позволяет формировать паттерны нормального поведения пользователей и обнаруживать отклонения от него как по классу пользователей, так и индивидуально для каждого. В результате классификации для каждого пользователя формируется рейтинг безопасности, который увеличивается с ростом числа отклонений от нормального поведения. По достижении определенного порога рейтинга безопасности система в автоматическом режиме оповещает администратора безопасности о возможном инциденте, связанном с воздействием внутреннего злоумышленника.

Применение в алгоритме генеративно-состязательной сети дает возможность генерировать дополнительные синтетические данные поведения пользователя с исходным распределением, что сокращает время, необходимое для сбора и подготовки исход-

ных данных. Как следствие, это уменьшает время, необходимое для внедрения такого решения в существующую систему защиты информации.

Процесс состязания двух нейронных сетей позволяет достичь высоких значений точности классификации с использованием дискриминатора благодаря адаптации модели к задаче обнаружения аномалий в данных, а внедрение иммунного алгоритма оптимизации способствует подбору оптимальных гиперпараметров модели машинного обучения для конкретной автоматизированной системы, учитывая особенности поведения всех пользователей.

Список источников

1. Барабанов Д. А., Иванова Т. А., Гараев Р. А. Перспективы применения и сценарии использования анализа поведения пользователей в сфере информационной безопасности // Информационные технологии интеллектуальной поддержки принятия решений. 2019. Т. 1. С. 202–206.

2. Абрамова О. Ф. Визуализация паттерна поведения пользователя web-системы // Кибернетика и программирование. 2019. № 3. С. 43–52. DOI: 10.25136/2644-5522.2019.3.23017.

3. Беззатеев С. В., Елина Т. Н., Мыльников В. А., Лившиц И. И. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Науч.-техн. вестн. информац. технологий, механики и оптики. 2021. Т. 21. № 4. С. 553–561. DOI: 10.17586/2226-1494-2021-21-4-553-561.

4. Ковалёв С. П., Калугина М. А. Комбинация алгоритмов K-средних и DBSCAN при анализе поведения пользователей // Студенческий (электрон. науч. журн.). 2019. № 18 (62). С. 33–38. URL: https://sibac.info/journal/student/62/140295 (дата обращения: 15.05.2019).

5. Козин И. С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе на основе анализа поведения пользователей // Информационно-управляющие системы. 2018. № 3. С. 69–78. DOI: 10.15217/1684-8853.2018.3.69.

6. Левковец Д. В., Алексеев И. В., Касаткин Д. П., Гурский С. М. Аутентификация пользователей на основе поведения на мобильных устройствах в различных контекстах использования // Вестн. науки. 2023. № 7 (64). С. 211–220.

7. Саенко И. Б., Котенко И. В., Аль-Барри М. Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопр. кибербезопасности. 2022. № 2 (48). С. 87–94.

8. Машечкин И. В. Исследование и разработка инновационной технологии построения программных средств обеспечения компьютерной безопасности, основанных на использовании методов машинного обучения и математической статистики для анализа данных поведенческой биометрии пользователей при работе в рамках стандартного человеко-машинного интерфейса, для решения задач активной аутентификации и идентификации пользователей, обнаружения внутренних вторжений и предотвращения попытки хищения конфиденциальной информации: отчет о прикладных научных исследованиях. М.: Изд-во МГУ, 2016. 205 с.

9. Трунов Е. Е. Исследование источников данных о пользователе для формирования модели поведенческого анализа с целью предупреждения внутренних угроз нарушения безопасности информации // Охрана, безопасность, связь. 2024. № 9-3. С. 111–118.

10. Шабанов А. А. Алгоритмы искусственной иммунной системы в интервальных методах глобальной оптимизации: выпуск. квалификац. работа. Новосибирск: Изд-во НГУ, 2016. 51 с.

11. Лебедев Б. К., Лебедев О. Б., Лебедева Е. О., Нагабедян А. А. Гибридный роевой алгоритм глобальной оптимизации в аффинном пространстве поиска // Программные продукты, системы и алгоритмы. 2019. Т. 1. С. 11–16.

12. Свидетельство о гос. регистрации программы для ЭВМ № 2025661274 Российская Федерация. Программа параметрической оптимизации гиперпараметров модели машинного обучения на основе алгоритма искусственной иммунной системы / Трунов Е. Е.; заявл. 27.04.2025: опубл. 05.05.2025.

13. ГОСТ Р 59898-2021. Оценка качества систем искусственного интеллекта. М.: Стандартинформ, 2021. 24 с.

14. IBM QRadar User Behavior Analytics. URL: https://www.ibm.com/ru-ru/marketplace/qradar-user-behavior-analytics (дата обращения: 10.10.2024).

15. Solar Dozor User Behavior Analytics. URL: https://rt-solar.ru/products/solar_dozor (дата обращения: 11.10.2024).

16. InfoWatch Prediction. URL: https://www.infowatch.ru/products/uba-sistema-prediction (дата обращения: 15.10.2024).

17. R-vision UEBA. URL: https://rvision.ru/products/ueba (дата обращения: 15.10.2024).

References

1. Barabanov D. A., Ivanova T. A., Garaev R. A. Perspektivy primeneniia i stsenarii ispol'zovaniia analiza povedeniia pol'zovatelei v sfere informatsionnoi bezopasnosti [Application prospects and scenarios for the use of user behavior analysis in the field of information security]. *Informatsionnye tekhnologii intellektual'noi podderzhki priniatiia reshenii*, 2019, vol. 1, pp. 202-206.

2. Abramova O. F. Vizualizatsiia patterna povedeniia pol'zovatelia web-sistemy [Visualization of the web system user behavior pattern]. *Kibernetika i programmirovanie*, 2019, no. 3, pp. 43-52. DOI: 10.25136/2644-5522.2019.3.23017.

3. Bezzateev S. V., Elina T. N., Myl'nikov V. A., Livshits I. I. Metodika otsenki riskov informatsionnykh sistem na osnove analiza povedeniia pol'zovatelei i intsidentov informatsionnoi bezopasnosti [Methodology for risk assessment of information systems based on the analysis of user behavior and information security incidents]. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2021, vol. 21, no. 4, pp. 553-561. DOI: 10.17586/2226-1494-2021-21-4-553-561.

4. Kovalev S. P., Kalugina M. A. Kombinatsiia algoritmov K-srednikh i DBSCAN pri analize povedeniia pol'zovatelei [A combination of K-means and DBSCAN algorithms

for analyzing user behavior]. *Studencheskii (elektronnyi nauchnyi zhurnal)*, 2019, no. 18 (62), pp. 33-38. Available at: https://sibac.info/journal/student/62/140295 (accessed: 15.05.2019).

5. Kozin I. S. Metod obespecheniia bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnoi sisteme na osnove analiza povedeniia pol'zovatelei [A method of ensuring the security of personal data during their processing in an information system based on an analysis of user behavior]. *Informatsionno-upravliaiushchie sistemy*, 2018, no. 3, pp. 69-78. DOI: 10.15217/1684-8853.2018.3.69.

6. Levkovets D. V., Alekseev I. V., Kasatkin D. P., Gurskii S. M. Autentifikatsiia pol'zovatelei na osnove povedeniia na mobil'nykh ustroistvakh v razlichnykh kontekstakh ispol'zovaniia [User authentication based on behavior on mobile devices in various usage contexts]. *Vestnik nauki*, 2023, no. 7 (64), pp. 211-220.

7. Saenko I. B., Kotenko I. V., Al'-Barri M. Kh. Primenenie iskusstvennykh neironnykh setei dlia vyiavleniia anomal'nogo povedeniia pol'zovatelei tsentrov obrabotki dannykh [The use of artificial neural networks to detect abnormal behavior of data center users]. *Voprosy kiberbezopasnosti*, 2022, no. 2 (48), pp. 87-94.

8. Mashechkin I. V. *Issledovanie i razrabotka innovatsionnoi tekhnologii postroeniia programmnykh sredstv obespecheniia komp'iuternoi bezopasnosti, osnovannykh na ispol'zovanii metodov mashinnogo obucheniia i matematicheskoi statistiki dlia analiza dannykh povedencheskoi biometrii pol'zovatelei pri rabote v ramkakh standartnogo chelovekomashinnogo interfeisa, dlia resheniia zadach aktivnoi autentifikatsii i identifikatsii pol'zovatelei, obnaruzheniia vnutrennikh vtorzhenii i predotvrashcheniia popytki khishcheniia konfidentsial'noi informatsii: otchet o prikladnykh nauchnykh issledovaniiakh* [Research and development of an innovative technology for building computer security software based on the use of machine learning methods and mathematical statistics to analyze user behavioral biometrics data when working within a standard human-machine interface, to solve problems of active user authentication and identification, detect internal intrusions and prevent attempts to steal confidential information: report on applied scientific research research]. Moscow, Izd-vo MGU, 2016. 205 p.

9. Trunov E. E. Issledovanie istochnikov dannykh o pol'zovatele dlia formirovaniia modeli povedencheskogo anali-za s tsel'iu preduprezhdeniia vnutrennikh ugroz narusheniia bezopasnosti informatsii [Research of data sources about the user to form a behavioral analysis model in order to prevent internal threats to information security]. *Okhrana, bezopasnost', sviaz'*, 2024, no. 9-3, pp. 111-118.

10. Shabanov A. A. *Algoritmy iskusstvennoi immunnoi sistemy v interval'nykh metodakh global'noi optimizatsii: vypusknaia kvalifikatsionnaia rabota* [Algorithms of the artificial immune system in interval methods of global optimization: final qualification work]. Novosibirsk, Izd-vo NGU, 2016. 51 p.

11. Lebedev B. K., Lebedev O. B., Lebedeva E. O., Nagabedian A. A. Gibridnyi roevoi algoritm global'noi optimizatsii v affinnom prostranstve poiska [Hybrid swarm algorithm for global optimization in an affine search space]. *Programmnye produkty, sistemy i algoritmy*, 2019, vol. 1, pp. 11-16.

12. Trunov E. E. *Programma parametricheskoi optimizatsii giperparametrov modeli mashinnogo obucheniia na osnove algoritma iskusstvennoi immunnoi sistemy* [A program for parametric optimization of hyperparameters of a machine learning model based on an artificial immune system algorithm]. Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM № 2025661274 Rossiiskaia Federatsiia; 05.05.2025.

13. GOST R 59898-2021. *Otsenka kachestva sistem iskusstvennogo intellekta* [ISS R 59898-2021. Quality assessment of artificial intelligence systems]. Moscow, Standartinform Publ., 2021. 24 p.

14. *IBM QRadar User Behavior Analytics*. Available at: https://www.ibm.com/ru-ru/marketplace/qradar-user-behavior-analytics (accessed: 10.10.2024).

15. *Solar Dozor User Behavior Analytics*. Available at: https://rt-solar.ru/products/solar_dozor (accessed: 11.10.2024).

16. *InfoWatch Prediction*. Available at: https://www.infowatch.ru/products/uba-sistema-prediction (accessed: 15.10.2024).

17. *R-vision UEBA*. Available at: https://rvision.ru/products/ueba (accessed: 15.10.2024).

Статья поступила в редакцию 04.05.2025; одобрена после рецензирования 28.07.2025; принята к публикации 21.10.2025
The article was submitted 04.05.2025; approved after reviewing 28.07.2025; accepted for publication 21.10.2025

Информация об авторе / Information about the author

Евгений Евгеньевич Трунов – адъюнкт кафедры защиты информации от несанкционированного доступа; Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко; ittehnology2018@gmail.com

Evgeny E. Trunov – Postgraduate Student of the Department of Protection of Information from Unauthorized Access; Krasnodar Higher Military awarded by the Orders of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S. M. Shtemenko; ittehnology2018@gmail.com