УДК 004.942

Иванова Юлия Павловна,
студент 2 курса, институт вычислительной математики и информационных технологий
Казанский (Приволжский) федеральный университет
Россия, г. Казань
Научный руководитель: Хайруллина Лилия Эмитовна

ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ УКРАДЕННЫХ УЧЕТНЫХ ДАННЫХ В ОНЛАЙН-СЕРВИСАХ НА ОСНОВЕ АНАЛИЗА ГЕТЕРОГЕННОГО ГРАФА СОБЫТИЙ АВТОРИЗАЦИИ

Аннотация: *В статье рассматривается задача обнаружения несанкционированного использования украденных учетных данных пользователей в онлайн-сервисах. Предложен метод на основе гетерогенного графа событий авторизации, узлы которого соответствуют пользователям, устройствам, IP-адресам и событиям входа. Для выявления аномалий разработана система из десяти пороговых правил, опирающаяся на тринадцать структурных признаков графа. Дополнительно проведён анализ вычислительной сложности, показавший, что замена промежуточной центральности степенной центральностью сокращает время обработки в 3.5 раза при снижении F1-score лишь на 0.018.*

Ключевые слова: *гетерогенный граф, обнаружение аномалий, учетные данные, credential stuffing, графовый анализ, информационная безопасность, пороговые правила.*

Annotation: *This paper addresses the problem of detecting unauthorized use of stolen user credentials in online services. A method based on a heterogeneous authorization event graph is proposed, whose nodes represent users, devices, IP*

addresses, and login events. A system of ten threshold rules relying on thirteen structural graph features is developed for anomaly detection. The proposed method outperformed the baseline by 25.6 p.p. in F1-score. An additional computational complexity analysis showed that replacing betweenness centrality with degree centrality reduces processing time by 3.5× with only a 0.018 decrease in F1-score.

Key words: *heterogeneous graph, anomaly detection, credentials, credential stuffing, graph analysis, information security, threshold rules.*

Введение

В современных онлайн-сервисах учетные записи пользователей являются одной из основных целей кибератак. Распространение утечек персональных данных ведёт к массовому использованию злоумышленниками скомпрометированных учетных данных – в частности, посредством атак типа credential stuffing, при которых автоматизированные инструменты проверяют миллионы пар «логин – пароль» на различных ресурсах [1, 2]. Особую сложность для обнаружения представляют атаки, в ходе которых злоумышленник предъявляет корректные учетные данные: традиционные механизмы проверки подлинности в этом случае не сигнализируют о компрометации.

Существующие методы обнаружения атак преимущественно анализируют отдельные события авторизации или статистические характеристики активности [3]. Однако они игнорируют структуру взаимосвязей между объектами системы (пользователями, устройствами и IP-адресами), что снижает их эффективность при выявлении сложных скоординированных атак [4].

В данной работе предлагается подход, основанный на гетерогенной графовой модели событий авторизации. Граф формализует связи между всеми объектами системы, а выявление аномалий выполняется путём анализа структурных характеристик этого графа. Это позволяет обнаруживать

паттерны, невидимые при поэлементном анализе: например, использование одного устройства для доступа ко множеству аккаунтов или массовые подключения с одного IP-адреса [5].

Обзор существующих работ

Обнаружение аномалий в информационных системах является хорошо изученной областью [3]. Классические подходы включают правиловые системы, статистические методы и методы машинного обучения. Их общее ограничение – рассмотрение событий как независимых сущностей без учёта взаимосвязей между ними.

Графовые методы анализа, активно развивающиеся в последнее десятилетие, позволяют преодолеть это ограничение [4]. Применительно к задачам кибербезопасности они используются для обнаружения мошенничества [6], выявления веб-роботов [7] и анализа аномальных связей в журналах авторизации [5].

Обзор гетерогенных графовых нейронных сетей для обнаружения аномалий в кибербезопасности [8] показывает, что гетерогенные графовые модели обеспечивают более высокую точность по сравнению с однородными, поскольку явно учитывают различные типы объектов и связей. Применение графового федеративного обучения для предсказания риска credential stuffing [9] демонстрирует перспективность подхода для задач, связанных с защитой учетных данных.

Тем не менее применение пороговых правил на основе структурных характеристик гетерогенного графа для обнаружения несанкционированного использования учетных данных остаётся недостаточно изученным, что определяет актуальность настоящего исследования.

Модель представления данных

Пользовательская активность представляется в виде ориентированного гетерогенного графа G = (V, E), где V – множество вершин, E – множество

рёбер. Множество вершин разбивается на пять непересекающихся подмножеств:

$$V = Vu \cup Vd \cup Vip \cup Vs \cup Vl,$$

где Vu – пользователи, Vd – устройства, Vip – IP-адреса, Vs – сессии, Vl – события авторизации. Рёбра кодируют конкретные взаимодействия: User → LoginEvent (пользователь инициировал вход), LoginEvent → Device (вход выполнен с устройства), LoginEvent → IP (вход выполнен с IP-адреса).

Для анализа пользовательской активности вычисляются тринадцать структурных признаков: количество событий авторизации, число уникальных устройств (n_devices) и IP-адресов (n_ips), доля неудачных попыток (failure_rate), индексы совместного использования устройств и IP (device_sharing, ip_sharing), энтропия IP-адресов (ip_entropy), burst score (минимальный интервал между событиями), степень вершины, промежуточная центральность пользователя и максимальная центральность связанных устройств и IP-адресов.

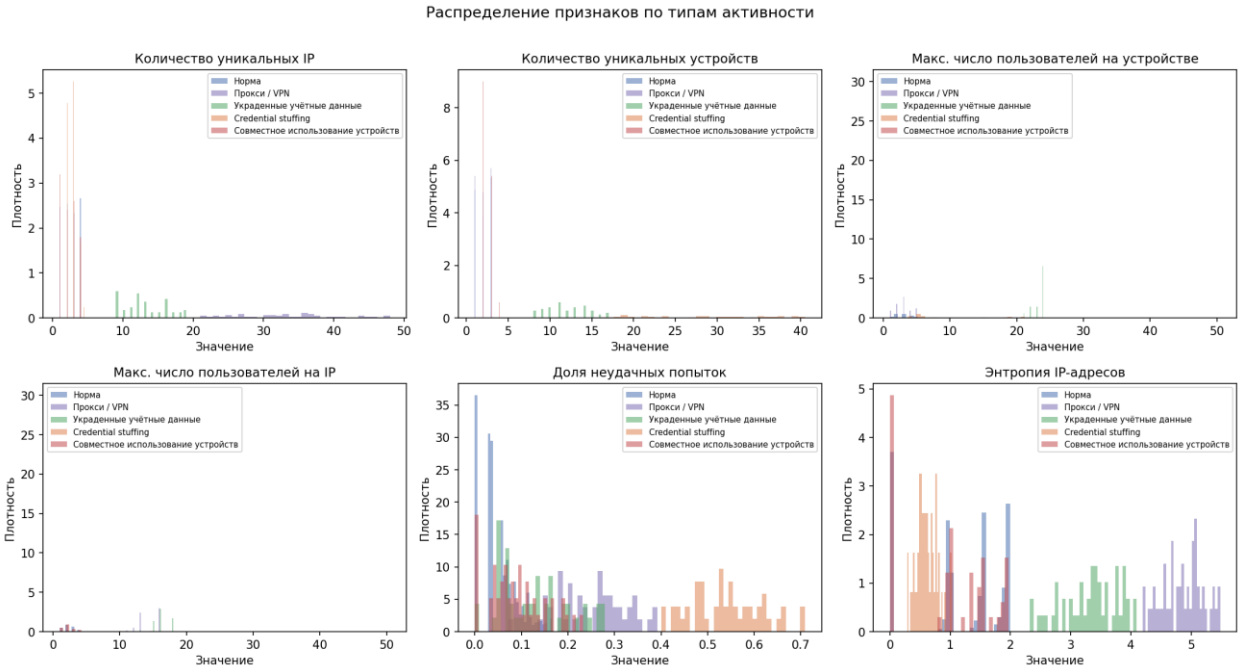

Рисунок 1. Распределение ключевых признаков по типам активности

Предлагаемый метод

Метод включает пять последовательных этапов: сбор журналов событий, построение гетерогенного графа, вычисление структурных признаков, применение пороговых правил и формирование списка подозрительных учетных записей.

Для принятия решения об аномальности учетной записи разработана система из десяти пороговых правил. Пороги определяются как процентили распределения признаков по всей выборке, что обеспечивает адаптивность метода к конкретным данным. Итоговое решение принимается по следующему правилу: учетная запись признаётся аномальной, если сработало два или более правил ($score \geq 2$), либо если значение *device_sharing* превышает 99-й перцентиль (усиленное правило для атак совместного использования устройств).

Таблица 1.

Правила обнаружения аномалий

Правило	Условие срабатывания	Выявляемая угроза
rule_many_ips	n_ips > 95-й перцентиль	Proxy/VPN, credential stuffing
rule_many_devices	n_devices > 95-й перцентиль	Stolen credentials
rule_device_sharing	device_sharing > 85-й перцентиль	Device sharing
rule_ip_sharing	ip_sharing > 90-й перцентиль	Credential stuffing
rule_high_failure	failure_rate > 95-й перцентиль	Brute force
rule_high_entropy	ip_entropy > 95-й перцентиль	Proxy/VPN
rule_burst	burst_score < 5 сек	Автоматизированные атаки
rule_high_betweenness	betweenness > 95-й перцентиль	Все типы
rule_device_centrality	max_dev_centrality > 90-й перцентиль	Device sharing

rule_ip_centrality	max_ip_centrality > 90-й перцентиль	Credential stuffing

Экспериментальное исследование

Для оценки эффективности метода сформирован синтетический набор данных, воспроизводящий реальные сценарии пользовательской активности. Каждое событие авторизации описывается кортежем (user_id, device_id, ip_address, timestamp, login_result).

Параметры набора данных: 2 000 пользователей (1 800 нормальных и 200 атакующих – 10 %), 61 462 события авторизации, 2 953 уникальных устройства, 3 620 уникальных IP-адреса. Граф пользовательской активности содержал 70 163 узла и 184 731 ребро [10].

Атакующие пользователи равномерно распределены по четырём типам атак (50 пользователей на каждый): credential stuffing (один IP-адрес обслуживает множество учетных записей), stolen credentials (вход с новых устройств и IP), device sharing (одно устройство для 50 аккаунтов) и proxy/VPN (20–50 разных IP-адресов для одного пользователя). Эталонная разметка формировалась на этапе генерации: метка 1 – скомпрометированная учетная запись, 0 – нормальная активность.

Результаты

Таблица 2.

Сводные результаты предложенного метода

Метрика	Предложенный метод	Базовый метод
Precision	0.987	0.743
Recall	0.775	0.520
F1-score	0.868	0.612
ROC-AUC	0.991	–

В качестве базового метода использовалось пороговое правило на основе числа неудачных попыток входа (90-й перцентиль). Предложенный метод превзошёл базовый по Precision на 24.4 п.п., по Recall на 25.5 п.п., по F1-score на 25.6 п.п.

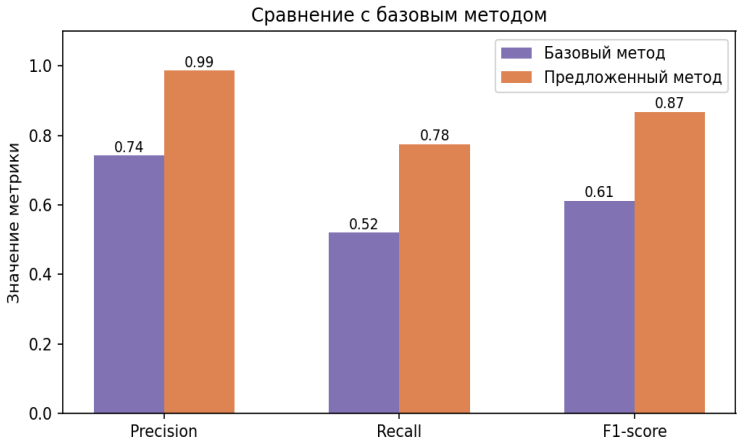

Рисунок 2. Сравнение предложенного и базового методов

Таблица 3.

Метрики качества по типам атак

Тип атаки	Precision	Recall	F1-score
Credential stuffing	0.980	1.000	0.990
Stolen credentials	0.980	1.000	0.990
Proxy/VPN	0.980	1.000	0.990
Device sharing	0.800	0.080	0.145

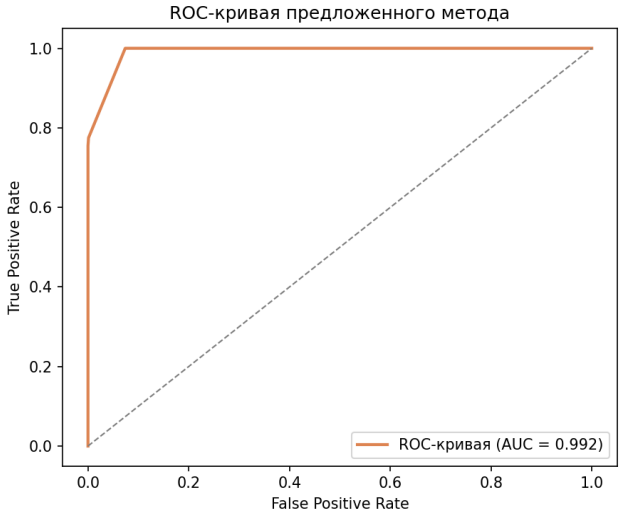

Рисунок 3. ROC-кривая предложенного метода (AUC = 0.991)

Обсуждение результатов

Предложенный метод демонстрирует высокую эффективность для трёх из четырёх типов атак (F1 = 0.990). Ключевое преимущество – учёт структуры взаимосвязей: атаки credential stuffing, stolen credentials и proxy/VPN формируют ярко выраженные графовые аномалии (высокое число IP-адресов, устройств или энтропия), которые надёжно обнаруживаются системой правил.

Существенно ниже показатели для атак device sharing (F1 = 0.145). Атакующие этой группы используют общее устройство лишь в части сессий, тогда как остальные их сессии характеризуются нормальным поведением – это не позволяет накопить достаточное число срабатываний правил. Данная проблема является направлением для дальнейшего совершенствования, в частности, посредством методов машинного обучения на графах [8].

Анализ вычислительной сложности выявил, что 91 % времени пайплайна (~34 с из ~50 с) занимает вычисление промежуточной центральности (betweenness, k = 500). Замена на degree centrality сокращает время до ~14 секунд (ускорение в 3.5×) при снижении F1 лишь на 0.018, что предпочтительно для систем реального времени.

Таблица 4.

Сравнение метрик центральности

Метрика центральности	Время (сек)	F1-score	ROC-AUC
Betweenness (k=500)	33.7	0.864	0.991
PageRank	0.40	0.846	0.995
Degree centrality	0.03	0.846	0.995

Заключение

В работе предложен метод обнаружения несанкционированного использования украденных учетных данных на основе анализа гетерогенного графа событий авторизации. Метод не требует размеченных обучающих данных и опирается на систему пороговых правил, адаптирующихся к характеристикам конкретного набора данных.

Экспериментальная проверка на синтетических данных подтвердила эффективность подхода: F1-score 0.868 и ROC-AUC 0.991 при превосходстве над базовым методом на 25.6 п.п. Выявленное ограничение по классу device sharing и узкое место вычислительной сложности определяют направления дальнейшей работы: интеграцию с методами Graph Neural Networks и применение degree centrality для развёртывания в режиме реального времени [8, 9].

Использованные источники:

1. Анализ уязвимостей в системах аутентификации пользователей: от классических атак до современных угроз [Электронный ресурс] // КиберЛенинка. – 2024. – URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-v-sistemah-autentifikatsii-polzovateley-ot-klassicheskih-atak-do-sovremennyh-ugroz (дата обращения: 12.03.2026).

2. Анализ уязвимостей и рисков традиционных парольных систем в контексте корпоративных распределённых систем [Электронный ресурс] //

КиберЛенинка. – 2025. – URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-i-riskov-traditsionnyh-parolnyh-sistem-v-kontekste-korporativnyh-raspredelennyh-sistem-i-kriticheski-vazhnyh (дата обращения: 15.03.2026).

3. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды ИСП РАН. – 2022. – Т. 34. – № 5. – С. 111–126. – DOI: 10.15514/ISPRAS-2022-34(5)-7.

4. Дадян Э.Г., Зеленков Ю.А. Методы, модели, средства хранения и обработки данных : учебник. – Москва : Вузовский учебник : ИНФРА-М, 2022. – 168 с.

5. Colhoun T., Torres A., Pacheco D. Detecting abnormal logins by discovering anomalous links via graph transformers // Computers & Security. – 2024. – Vol. 144. – Article 103975.

6. Liu Z., Dou Y., Yu P.S. Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection // Proceedings of the 43rd ACM SIGIR Conference. – 2020. – P. 1569–1572.

7. Менщиков А.А., Гатчин Ю.А. Метод обнаружения веб-роботов на основе анализа графа пользовательского поведения // Программные продукты и системы. – 2019. – Т. 32. – № 4. – С. 607–612. – DOI: 10.15827/0236-235X.128.607-612.

8. Jiang L., Ryan R., Li Q., Ferdosian N. A Survey of Heterogeneous Graph Neural Networks for Cybersecurity Anomaly Detection // arXiv preprint arXiv:2510.26307. – 2025.

9. Kim H. et al. PassREfinder-FL: Privacy-Preserving Credential Stuffing Risk Prediction via Graph-Based Federated Learning // Expert Systems with Applications. – 2025. – Vol. 281. – Article 126836.

10. Hagberg A.A., Schult D.A., Swart P.J. Exploring network structure, dynamics, and function using NetworkX // Proceedings of the 7th Python in Science Conference. – Pasadena, 2008. – P. 11–15.