www.volsu.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
В БЕЗОПАСНОСТИ И ТЕЛЕКОММУНИКАЦИЯХ

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.1.1

УДК 004.775
ББК 32.972.53

МЕТОДЫ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Светлана Александровна Елизарова

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
bit-211_114288@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент, кафедра информационной безопасности,
Волгоградский государственный университет
babenko.aleksey@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Проанализирована статистика угроз поведения пользователей в информационных системах. Определена процедура анализа поведения пользователей в информационной системе. Представлена классификация методов анализа поведения пользователей в информационных системах. Для выявления наиболее эффективного метода анализа поведения пользователей в информационных системах определены критерии для их сравнения. Приведен результат сравнения методов анализа поведения пользователей в информационной системе по выделенным критериям.

Ключевые слова: информационная безопасность, внутренний нарушитель, анализ поведения пользователей, анализ последовательности событий, анализ аномалий.

© Елизарова С.А., Бабенко А.А., 2025

В свете растущей угрозы кибератак современный подход к защите данных в компаниях меняется. Основной акцент смещается на внедрение технических барьеров: межсетевых экранов, антивирусных решений и систем анализа трафика. Тем не менее недостаточное внимание уделяется человеческому фактору, который включает непроизвольные ошибки сотрудников, пренебрежение стандартными правилами работы с данными и умыш-

ленные злонамеренные действия, включая социальную инженерию. Около 79 % случаев утечки персональной информации происходит из-за действий людей внутри организаций – как в результате сознательного нарушения, так и по незнанию или недостатку профессиональных навыков [4].

На рисунке 1 представлены статистические данные компании Positive Technologies за 3-й квартал 2024 г., представляющие наиболее распространенные методы атак нарушителей на информационные системы [1].

Исходя из этого, можно сделать вывод о том, что угрозы информационной безопасности по вине пользователя системы являются частым явлением, а среди наиболее распространенных методов атак выделяются социальная инженерия и использование ВПО.

Для эффективного противостояния динамично развивающимся угрозам критически важно внедрение комплексных мер управления информационной безопасностью. Особое значение приобретает анализ поведения пользователей, позволяющий выявлять нетипичные действия и предотвращать инциденты на ранних стадиях. Такой подход способствует более эффективному реагированию на угрозы и разработке стратегий повышения устойчивости корпоративной безопасности.

Под анализом поведения пользователей в информационной системе понимается комплекс действий по сбору данных о конкретных действиях пользователей при использовании компьютерной инфраструктуры, включая последующую их обработку для выявления закономерностей взаимодействия с различными приложениями, интернет-порталами и сервисными ресурсами. Задача этого процесса заключается в глубоком осознании механизмов поведения клиентов по отношению к программным продуктам и предлагаемым услугам.

Данный анализ может охватывать следующие ключевые моменты:

1. Сбор и обработка данных об активности пользователей – информация о всех действиях пользователей в рамках работы на компьютере, включая запуск программного обеспечения, электронную почтовую переписку, посещение веб-ресурсов.

2. Аналитическая оценка собранных сведений – выявление структурных особенностей и системных закономерностей в поведении пользователей во время взаимодействия с компьютерными системами.

3. Применение аналитических результатов – использование статистических выводов, полученных из анализа данных, для оптимизации работы как самих пользователей, так и всей информационной инфраструктуры.

4. Распознавание аномального поведения – выявление отклонений в обычной активности пользователей при работе с компьютерами, что способствует обнаружению потенциальных проблем или нарушений в функционировании системы.

Использование различных методов анализа поведения пользователей в информационных системах помогает выявлять аномалии и подозрительные действия. Такие методы

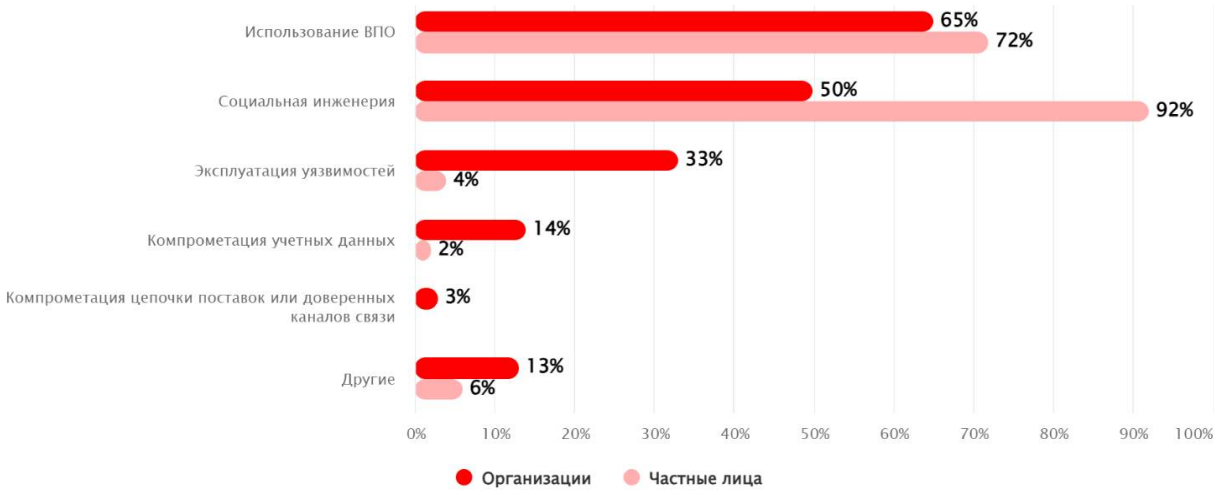


Рис. 1. Статистика использования методов атак на информационные системы

могут анализировать различные аспекты поведения пользователей, включая их взаимодействие с системой, действия в сети, доступ к данным и другие параметры.

Классификация методов, используемых для анализа поведения пользователей, представлена на рисунке 2.

Анализ аномалий используется для выявления отклонений от нормального поведения пользователей и включает следующие основные методы [3]:

1. Статистический анализ: метод анализирует нормальные статистические характеристики поведения (например, частота логинов, объем передаваемых данных) и на основе этих данных строит модель нормального поведения. Когда поведение пользователя выходит за пределы этих норм, оно считается аномальным.

2. Методы кластеризации: например, k-средних (k-means) или DBSCAN. Этот метод группирует пользователей по схожести их поведения, а затем выделяет пользователей, чье поведение сильно отличается от большинства.

3. Методы машинного обучения: Использование алгоритмов обучения без учителя (например, автоэнкодеры, SVM с ядром) для выявления отклонений от нормального поведения.

Методы анализа последовательности событий исследуют, как действия пользователей развиваются во времени [5]:

1. Марковские модели (Hidden Markov Models) используются для анализа последовательности событий, например, для отслеживания логинов, доступа к данным и изменений настроек. Модели предсказывают, какие следующие действия могут быть совершены пользователем, и выявляют отклонения, если происходят неожиданные переходы.

2. Алгоритмы поиска ассоциаций, например, Apriori или FP-growth, используются для выявления скрытых закономерностей между действиями пользователей, например, какие операции часто выполняются в комбинации, что может указать на аномалии.

Методы классификации используются для предсказания типа поведения пользователя на основе исторических данных о действиях [7]:

1. Логистическая регрессия и деревья решений используются для классификации действий пользователя как «нормальные» или «подозрительные», основываясь на заранее подготовленных признаках.

2. Random Forest и градиентный бустинг могут комбинировать несколько простых классификаторов и принимать решения на основе большинства голосов. Они хорошо подходят для более сложных случаев, когда взаимодействие между признаками не линейное.

Метод анализа сетевых взаимодействий рассматривает поведение пользователей в контексте их взаимодействий с другими пользователями или системами [8]:

1. Графовые алгоритмы – алгоритмы, использующие графы для моделирования взаимосвязей между пользователями, могут ис-

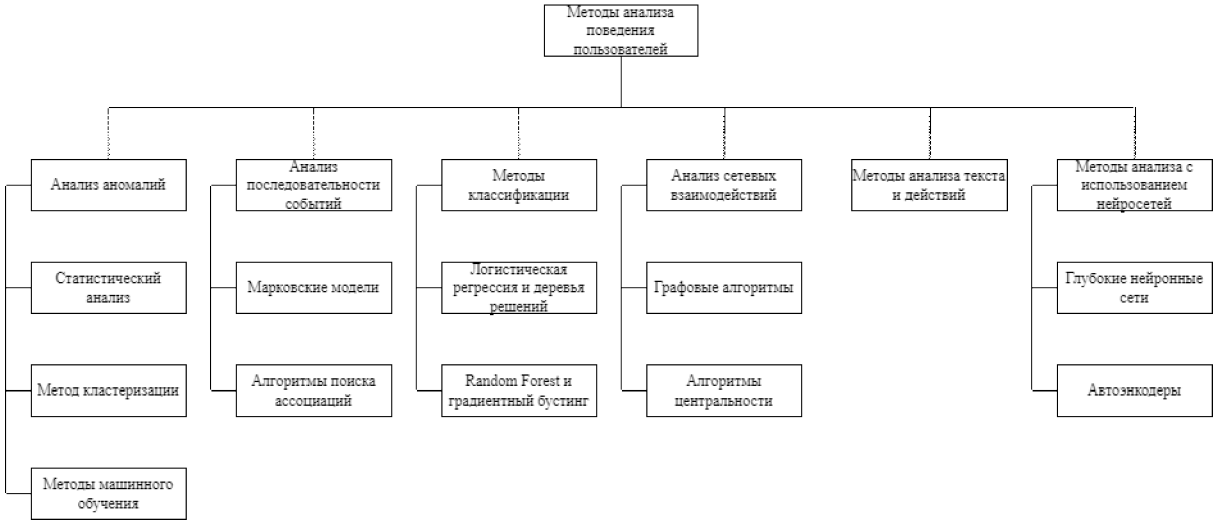


Рис. 2. Классификация методов анализа поведения пользователей

пользоваться для выявления аномальных структур, таких как попытки пользователями создать необычные связи или манипулировать системой.

2. Алгоритмы центральности, например PageRank, HITS, помогают выделить ключевых пользователей в системе на основе их активности и взаимодействий с другими пользователями.

Если система генерирует журналы или текстовую информацию, например, сообщения, комментарии, логи, то метод анализа текста может быть использован для обнаружения подозрительных или аномальных действий. Примером может послужить анализ сообщений, отправляемых через внутреннюю корпоративную систему на наличие фраз, которые могут указывать на попытки мошенничества или утечку информации [2].

Методы анализа с использованием нейросетей подразделяются на [6]:

1. Глубокие нейронные сети (Deep Learning): они могут быть использованы для более сложного анализа поведения, когда необходимо работать с большими объемами данных или выявлять скрытые закономерности. Применяются в задачах анализа последовательностей действий или изображений (например, анализ видеонаблюдения за рабочими процессами).

2. Автоэнкодеры: для поиска аномалий и редких событий можно использовать автоэнкодеры, которые обучаются на «нормальных» данных, а затем выявляют отклонения, которые могут свидетельствовать о нарушении безопасности.

Методы анализа поведения пользователей могут быть использованы в различных контекстах для повышения безопасности и улучшения мониторинга. Наиболее эффективные методы часто комбинируют несколько подходов, чтобы создать комплексную систему защиты, способную обнаруживать как простые аномалии, так и более сложные, скрытые угрозы.

Для сравнения методов анализа поведения пользователей с целью выявления наиболее эффективного, определим следующие критерии оценки и их возможные значения (табл. 1).

Где показатели равны: высокая – 0, средняя – 0,5, низкая – 1.

Эти критерии оценки помогут оценить методы анализа поведения пользователей в информационных системах и выбрать вариант, который обеспечит наиболее эффективную защиту.

Для использования метода Евклидова расстояния в оценке методов анализа поведения пользователей нам потребуется определить числовые значения для каждого решения и критерия, а затем вычислить расстояния между ними.

Шаги для расчета методом Евклидова расстояния:

1. Определим критерии оценки для методов анализа поведения пользователей:

Критерий 1 – Точность результатов.

Критерий 2 – Сложность реализации.

Критерий 3 – Адаптивность.

Критерий 4 – Время обучение.

Критерий 5 – Полнота анализа.

2. Присвоим числовые значения каждому критерию, отражающие его уровень в методах анализа поведения пользователей.

Таблица 1

Критерии для сравнения методов анализа поведения пользователей в ИС

№ Критерия	Обозначение	Название	Описание	Возможное значение
1	2	3	4	5
1	К1	Точность результатов	Оценка способности метода выявлять аномалии или правильно классифицировать поведение пользователя	Высокая, Низкая
2	К2	Сложность реализации	Легкость внедрения метода в существующую инфраструктуру	Высокая, Низкая
3	К3	Адаптивность	Способность метода адаптироваться к изменению поведения пользователей со временем	Высокая, Средняя, Низкая
4	К4	Время обучения	Время, необходимое для первоначального обучения модели, использующих машинное обучение	Высокая, Низкая
5	К5	Полнота анализа	Способность метода учитывать различные аспекты поведения пользователей и их взаимодействие с системой	Высокая, Низкая

3. Создадим таблицу соответствия методов анализа поведения пользователей заданным критериям (табл. 2) и для каждого подхода вычислим расстояние методом Евклида, используя значения критериев по формуле.

$$E = \sqrt{(1-К1)^2 + (1-К2)^2 + (1-К3)^2 + \\ + (1-К4)^2 + (1-К5)^2}$$

После вычисления расстояний для всех методов нужно сравнить их значения. Здесь меньшее значение расстояния указывает на более эффективную работу методов анализа поведения пользователей.

Ниже представлена диаграмма с результатами сравнения эффективности методов анализа поведения пользователей (рис. 3).

Исходя из полученных результатов, мы можем сделать вывод о том, что анализ последовательности событий является самым эффективным методом анализа поведения пользователей в ИС из рассматриваемых вариантов.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: III квартал 2024 года // Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id19

2. Анализ поведения пользователей с помощью методов интернет-маркетинга // ScienceProblems. – URL: https://scienceproblems.ru/analiz-povedenija-polzovatele.html

3. Системы анализа поведения пользователей (UBA – User Behavior Analytics) – Сравнение и вы-

Таблица 2

Значение и оценки методов анализа поведения пользователей

№ метода анализа	Метод анализа	Критерии					Результат
1	2	3					4
		К1	К2	К3	К4	К5	
1	Анализ аномалий	1	1	1	0	0	1,41
2	Анализ последовательности событий	1	1	1	1	1	0
3	Методы классификации	0	0	0	0	0	2,24
4	Анализ сетевых взаимодействий	0	0	0,5	0	0	2,06
5	Методы анализа текста и действий	0	0	0,5	0	0	2,06
6	Методы анализа с использованием нейросетей	1	0	1	0	0	1,73

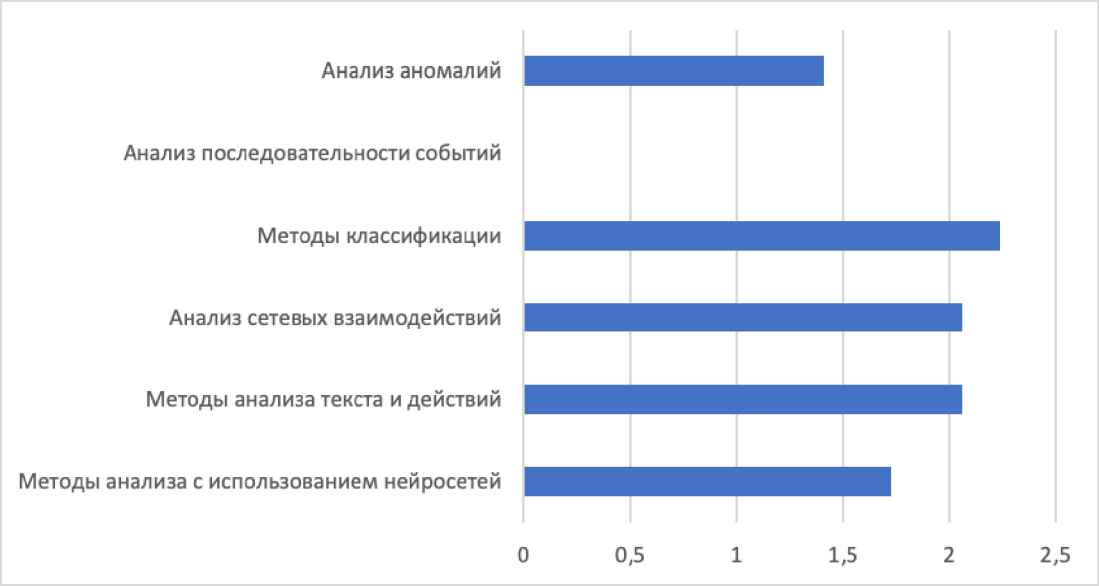


Рис. 3. Результаты сравнительного анализа

бор // Anti-Malware. – URL: https://www.anti-malware.ru/security/user-behavior-analytics

4. Утечка персональных данных: законы и штрафы // Forus. – URL: https://forus.ru/about/news/utechka-personalnykh-dannykh-zakony-i-shtrafy/

5. COHORTNEY: Non-Parametric Clustering of Event Sequences / L. Liu [et al.] // arXiv. – 2021. – URL: https://arxiv.org/abs/2104.01440

6. M3A: Model, MetaModel, and Anomaly Detection in Web Searches / D.-C. Juan [et al.] // arXiv. – 2016. – P. 1–10. – DOI: 10.48550/arXiv.1606.05978

7. Profiling Users by Modeling Web Transactions / S. Y. Lee [et al.] // arXiv. – 2017. – URL: https://arxiv.org/abs/1703.09745

8. User Modeling Combining Access Logs, Page Content and Semantics / R.P. Liu [et al.] // arXiv. – 2011. – URL: https://arxiv.org/abs/1103.5002

REFERENCES

1. Aktualnye kiberugrozy: III kvartal 2024 goda [Current Cyber Threats: Q3 2024]. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id19

2. Analiz povedeniya polzovatelej s pomoshchyu metodov internet-marketinga [User Behavior Analysis Using Internet Marketing Methods]. *ScienceProblems*. URL: https://scienceproblems.ru/analiz-povedenija-polzovatele.html

3. Sistemy analiza povedeniya pol'zovatelej (UBA – User Behavior Analytics) – Sravnenie i vybor [User Behavior Analytics Systems – Comparison and Selection]. *Anti-Malware*. URL: https://www.anti-malware.ru/security/user-behavior-analytics

4. Utechka personalnyh dannyh: zakony i shtrafy [Leak of Personal Data: Laws and Fines]. *Forus*. URL: https://forus.ru/about/news/utechka-personalnykh-dannykh-zakony-i-shtrafy/

5. Liu L., Huo Y., Xie X. et al. COHORTNEY: Non-Parametric Clustering of Event Sequences. *arXiv*, 2021. URL: https://arxiv.org/abs/2104.01440

6. Juan D.-C., Shah N., Tang M. et al. M3A: Model, MetaModel, and Anomaly Detection in Web Searches. *arXiv*, 2016, pp. 1-10. DOI: 10.48550/arXiv.1606.05978

7. Lee S.Y., Liu R.P., Sandvik F.A.W. et al. Profiling Users by Modeling Web Transactions. *arXiv*, 2017. URL: https://arxiv.org/abs/1703.09745

8. Liu R.P., Lee S.Y., Sandvik F.A.W. et al. User Modeling Combining Access Logs, Page Content and Semantics. *arXiv*, 2011. URL: https://arxiv.org/abs/1103.5002

METHODS FOR ANALYZING USER BEHAVIOR IN INFORMATION SYSTEMS

Svetlana A. Elizarova

Student, Department of Information Security,
Volgograd State University
bit-211_114288@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Information Security,
Volgograd State University
babenko.aleksey@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article examines methods for analyzing user behavior in information systems, focusing on identifying anomalies and preventing security threats. The authors highlight the growing risk of cyberattacks, emphasizing that 79% of data breaches result from human actions, whether intentional or accidental. Traditional security measures like firewalls and antivirus software are insufficient, necessitating advanced behavioral analysis to detect unusual activities early. The study presents a classification of methods for analyzing user behavior, including anomaly detection, event sequence analysis, classification techniques, network

interaction analysis, text analysis, and neural network-based approaches. Each method is evaluated based on criteria such as accuracy, implementation complexity, adaptability, training time, and comprehensiveness. The Euclidean distance metric is applied to compare these methods, revealing that event sequence analysis is the most effective for identifying deviations in user behavior. The findings underscore the importance of integrating multiple analytical approaches to enhance security systems. By combining methods like statistical analysis, machine learning, and graph algorithms, organizations can better detect both simple anomalies and complex threats. The article provides valuable insights for improving information security strategies, advocating for a proactive approach to mitigate risks posed by internal and external threats.

Key words: information security, internal intruder, analyzing user behavior, analyzing event sequence, anomaly analysis.