Инженерный вестник Дона, №6 (2025)
ivdon.ru/ru/magazine/archive/n6y2025/10135

Построение пространства атрибутов для оценки поведенческих аномалий при взаимодействии пользователей с CRM-системой

К.А. Хализев

Московский технический университет связи и информатики

Аннотация: В статье предложена методика построения пространства атрибутов для выявления поведенческих аномалий пользователей в системах управления взаимоотношениями с клиентами (system of customer relationship management или CRM-система). Описаны способы регистрации действий через встроенные трекеры, позволяющие фиксировать активность, клики, движения курсора и нажатия клавиш. Агрегация этих данных в векторы признаков обеспечивает применение алгоритмов машинного обучения для обнаружения нарушений и повышения информационной безопасности в CRM-системе.
Ключевые слова: информационная безопасность, CRM-система, поведенческий анализ, выявление аномалий, идентификация пользователей, аналитика поведения, мониторинг активности, цифровой след, инсайдерские угрозы, пространство атрибутов.

Введение

Современные системы управления отношениями с клиентами (system of customer relationship management или CRM-система) играют ключевую роль при построении бизнес-процессов компаний, обеспечивая централизованное управление продажами, маркетингом и обслуживанием клиентов. При этом каждый пользователь системы оставляет цифровой поведенческий след — последовательность действий, которая может многое рассказать о его намерениях, привычках и даже возможных нарушениях регламента. Обеспечение информационной безопасности таких систем, а также защита хранящейся в них информации становится ключевым фактором для поддержания деятельности компаний и приведения к нормам законодательства.

Поведенческий анализ пользователей в CRM позволяет решать широкий спектр задач: от выявления неэффективных бизнес-процессов до обнаружения аномальной активности, потенциально связанной с внутренними угрозами безопасности. Однако эффективный анализ возможен только при условии правильно сформированной структуры данных —

пространства атрибутов, способного адекватно описывать поведение пользователей.

Целью данной статьи является построение пространства атрибутов для оценки поведенческих аномалий при взаимодействии пользователей с CRM-системой. В качестве примера CRM-системы рассматривается реальная система Fitbase (fitbase.io), для нее описываются типовые сценарии использования, методы фиксации действий, а также способы хранения и представления собранных данных. Предлагаемое решение ориентировано на последующее применение в системах мониторинга и анализа поведения пользователей CRM-систем для обеспечения информационной безопасности и защиты хранящейся информации.

Типовые действия, выполняемые в CRM-системе на примере Fitbase

CRM-система Fitbase представляет собой специализированное облачное решение, предназначенное для автоматизации бизнес-процессов в индустрии фитнес-услуг: фитнес-клубах, танцевальных школах, студиях йоги и аналогичных организациях. Она включает в себя как веб-интерфейс, так и мобильные приложения, ориентированные на разные категории пользователей: администраторов, тренеров и клиентов.

Пользовательская активность в CRM Fitbase охватывает широкий спектр действий, каждое из которых оставляет цифровой след, потенциально пригодный для анализа. На рисунке 1 приведена классификация типовых сценариев взаимодействия пользователя с системой.

Все эти действия являются основой для построения пространства атрибутов и могут быть агрегированы по временным интервалам, что делает их пригодными для последующего анализа с помощью моделей машинного обучения.

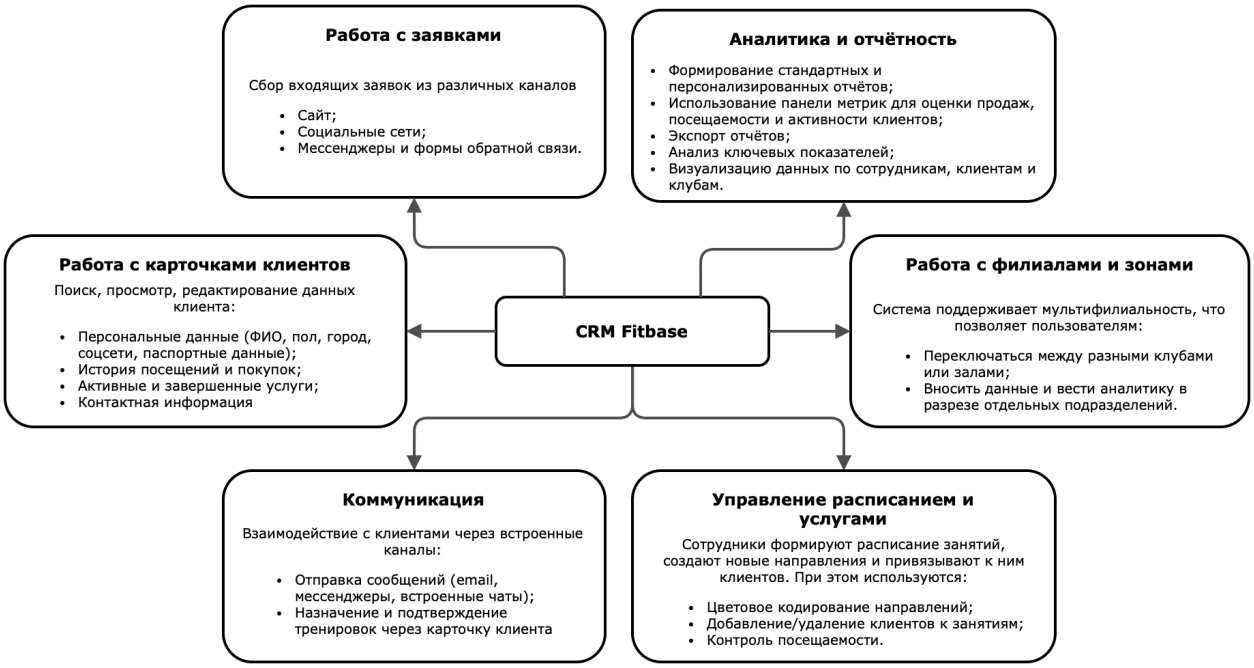

Рис. 1. – Схема сценариев взаимодействия клиента с CRM-системой

Способы фиксации действий пользователя в CRM-системе и обобщённые алгоритмы сбора данных

Сбор и фиксация пользовательской активности в CRM-системе реализуется с помощью системы трекеров, встраиваемой в интерфейс клиента. Эти трекеры функционируют как элементы клиентской логики и предназначены для регистрации действий пользователя в процессе его взаимодействия с системой. Подобный подход позволяет формировать детальные поведенческие профили сотрудников, что критически важно для задач аудита, обеспечения безопасности и выявления аномалий.

Система трекеров охватывает несколько ключевых категорий действий:

Общая активность пользователя — отслеживаются периоды активности во вкладке браузера, включая любые взаимодействия: перемещение курсора мыши, нажатия клавиш, прокрутка страницы и т.п.

Буфер обмена — фиксируются факты копирования информации в буфер, с возможностью последующего анализа содержимого на наличие персональных или конфиденциальных данных.

Нажатия кнопок и переходы по вкладкам интерфейса CRM-системы — регистрируются клики по элементам управления и пользовательская навигация в системе.

Сочетания клавиш — отслеживаются комбинации клавиш, включая горячие клавиши и потенциально подозрительные шаблоны (например, попытки копирования/вставки или вызова системных функций).

Каждое действие снабжается метаинформацией: временем совершения, контекстом (текущая страница, URL, роль пользователя, идентификатор клуба и т.д.), а также уникальным цифровым отпечатком пользователя, сформированным по данным устройства, с которого выполнен вход, и окружения.

Механизмы сбора построены на периодической агрегации в заданные временные интервалы (например, каждые 5 минут). На протяжении выбранного интервала агрегации система регистрирует все события определённого типа, после чего агрегирует их в обобщённую метрику:

- длительность активности и неактивности,
- количество взаимодействий (кликов, прокруток, нажатий),
- обнаруженные шаблоны копирования и передачи данных,
- частота и разнообразие комбинаций клавиш.

Полученные агрегаты сериализуются в структурированном формате (JSON) и передаются на серверную часть системы.

Итоговое представление вектора для хранения данных

В результате предварительной обработки и агрегации логов пользовательской активности (перемещения курсора и клики мышью, нажатия на клавиатуру, анализ содержимого буфера обмена, нахождение на вкладках и т.д.) каждый временной интервал пользовательского поведения представляется в виде вектора признаков фиксированной размерности. Такие векторы агрегируются по пятиминутным интервалам и привязываются к

конкретной вкладке (странице) CRM-системы, на которой происходили действия. Исследования подтверждают эффективность объединения поведенческой информации на уровне признаков для задач контекстной и непрерывной идентификации [1].

Каждый вектор включает в себя следующие ключевые метрики:

- Показатели активности: процент активности, средняя активность, количество открытий вкладки;
- Метрики клавиатурной активности: среднее время нажатия клавиш, средняя скорость ввода;
- Параметры перемещения курсора мыши и нажатия: средняя скорость и ускорение, количество кликов, скорость прокрутки;
- Сведения о буфере обмена: количество обнаруженных конфиденциальных данных/персональных данных, типы данных [2].

Все значения нормализуются с помощью стандартизации и приводятся к единому масштабу. В итоге формируется входной вектор размерности 10–11 признаков, представляющий обобщённую поведенческую модель пользователя за конкретный временной интервал на определённой вкладке CRM.

Выводы

Разработанное пространство атрибутов представляет собой универсальную основу для последующего анализа и интерпретации пользовательской активности в CRM-системах. Используя это пространство, открывается ряд перспектив в области информационной безопасности, прикладной аналитики и адаптивного управления доступом.

Во-первых, данное пространство атрибутов позволяет эффективно разрабатывать алгоритмы для выявления аномалий в поведении пользователей на основе алгоритмов машинного обучения, в частности автокодировщиков. Это особенно актуально в контексте противодействия

инсайдерским угрозам, где критическое значение имеет своевременное обнаружение отклонений от типового поведенческого профиля. Методы поведенческой аналитики всё чаще рассматриваются как основа для мониторинга и раннего выявления аномальной активности в киберпространстве [3, 4].

Во-вторых, на основе результатов, полученных в ряде исследований [5], можно утверждать, что поведенческие характеристики взаимодействия с пользовательским интерфейсом обладают высокой информативностью с точки зрения непрерывной идентификации. Эти подходы могут быть адаптированы к контексту CRM-систем, где фиксируются такие параметры, как скорость ввода, характер кликов и навигационные паттерны.

В-третьих, перспективным направлением является использование графовых моделей для анализа пользовательского поведения, в том числе с применением методов, основанных на анализе графлетов [6]. Применение таких моделей в CRM-среде позволяет выделять устойчивые поведенческие структуры и выявлять редкие или нетипичные сценарии взаимодействия. Такие подходы получили развитие и в управлении клиентскими взаимодействиями, включая CRM-системы, что подтверждается последними исследованиями в области графового моделирования [7].

Кроме того, в ряде современных работ подчёркивается влияние многозначности целевых меток и контекстуальных факторов на результаты классификации в системах мониторинга [8–10]. Это особенно важно при построении систем, где поведенческие данные имеют высокую степень вариативности в зависимости от роли пользователя, времени суток, выполняемых функций и других условий.

Таким образом, предложенное пространство атрибутов может служить не только инструментом для обнаружения аномалий и инцидентов, но и основой для создания интеллектуальных адаптивных систем поведенческого

анализа. Такие системы способны объединять принципы поведенческой биометрии, графовой интерпретации и контекстной многоклассовой классификации, что обеспечивает высокий уровень адаптивности и точности в задачах информационной безопасности.

Литература

1. Meng W., Wong D.S., Furnell S., Zhou J. Combining user behavioural information at the feature level to enhance continuous authentication: A systematic review // Knowledge-Based Systems. 2021. V. 214. P. 106728. URL: sciencedirect.com/science/article/pii/S0950705122002398

2. Шелухин О.И., Осин А.В., Костин Д.В. Мониторинг и диагностика аномальных состояний компьютерной сети на основе изучения “исторических данных” // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. №4. С. 23–30. DOI: 10.36724/2072-8735-2020-14-4-23-30

3. Torabi H., Mirtaheri, S.L., Greco, S. Practical autoencoder based anomaly detection by using vector reconstruction error // Cybersecurity. 2022. V. 5. pp. 1–19. URL: cybersecurity.springeropen.com/articles/10.1186/s42400-022-00134-9

4. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. 2009. V. 41. No. 3. pp. 1–58. URL: dl.acm.org/doi/10.1145/1541880.1541882

5. Осин А.В., Мурашко Ю.В., Суворов В.И. Поведенческие характеристики взаимодействия с сенсорным экраном для идентификации пользователей мобильных устройств // Инженерный вестник Дона. 2024. №12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9686

6. Хализев К.А., Осин А.В. Прогнозирование редких событий на основе анализа графлетов взаимодействия в социальных сетях // Инженерный вестник Дона. 2025. №4. URL: ivdon.ru/ru/magazine/archive/n4y2025/9986

7. Alves B., dos Santos M.A., de Souza J.M. A graph-based approach to client relationship management in fund management industry // Journal of Innovation &

Knowledge. 2022. V. 7. No. 3. P. 100175. URL: sciencedirect.com/science/article/pii/S2444569X22001081

8. Шелухин О.И., Раковский Д.И. Обучение с множественными метками в компьютерных сетях // Системы генерации и обработки сигналов в интересах бортовой связи. 2023. Т. 6. №1. URL: elibrary.ru/item.asp?id=54737401

9. Раковский Д.И. Анализ проблемы многозначности меток классов в безопасности компьютерных сетей // Synchroinfo Journal. 2022. Т. 8. №6. URL: elibrary.ru/item.asp?id=59270170

10. Раковский Д.И., Александров И.Д. Предобработка данных табличной структуры для решения задач многозначной классификации компьютерных атак // Инженерный вестник Дона. 2024. №12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9670

References

1. Meng W., Wong D.S., Furnell S., Zhou J. Knowledge-Based Systems. 2021. V. 214. P. 106728. URL: sciencedirect.com/science/article/pii/S0950705122002398

2. Sheluhin O.I., Osin A.V., Kostin D.V. T-Comm: Telecommunications and Transport. 2020. V. 14. No. 4. pp. 23–30. DOI: 10.36724/2072-8735-2020-14-4-23-30

3. Torabi H., Mirtaheri, S.L., Greco, S.Cybersecurity. 2022. V. 5. pp. 1–19. URL: cybersecurity.springeropen.com/articles/10.1186/s42400-022-00134-9

4. Chandola V., Banerjee A., Kumar V. ACM Computing Surveys. 2009. V. 41. No. 3. pp. 1–58. URL: dl.acm.org/doi/10.1145/1541880.1541882

5. Osin A.V., Murashko Y.V., Suvorov V.I. Inzhenernyj vestnik Dona. 2024. No. 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9686

6. Khalizev K.A., Osin A.V. Inzhenernyj vestnik Dona. 2025. No. 4. URL: ivdon.ru/ru/magazine/archive/n4y2025/9986

7. Alves B., dos Santos M.A., de Souza J.M. Journal of Innovation & Knowledge. 2022. V. 7. No. 3. P. 100175. URL: sciencedirect.com/science/article/pii/S2444569X22001081

8. Sheluhin O.I., Rakovskiy D.I. Systems of Signals Generating and Processing in the Field of on Board Communications. 2023. V. 6. No. 1. URL: elibrary.ru/item.asp?id=54737401

9. Rakovskiy D.I. Synchroinfo Journal. 2022. V. 8. No. 6. URL: elibrary.ru/item.asp?id=59270170

10. Rakovskiy D.I., Alexandrov I.D. Inzhenernyj vestnik Dona. 2024. No. 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9670.

Дата поступления: 10.04.25

Дата публикации: 25.05.2025