

УДК 004.056

E.V.Seroshtan, A.S. Sivova

THE ROLE OF BEHAVIORAL ANALYTICS TECHNOLOGY IN DETECTING INSIDER THREATS IN THE CORPORATE ENVIRONMENT

In this study, behavioral analytics is considered as a powerful tool for cybersecurity. The results of a theoretical study are presented, revealing the role of technology in identifying insider threats in the corporate environment. Current statistical data is analyzed, characterizing the dynamics of registered data leaks caused by internal violators both globally and in our country. The main types of insiders are identified, attention is drawn to behavioral indicators, and the strengths and weaknesses of behavioral analytics are shown, which should be taken into account when implementing it in the practice of Russian organizations in the context of compliance with the legal norms of the current legislation. The theoretical and practical value of the study lies in the generalization of relevant information and the possibility of using it to improve the security of confidential information from insider threats.

Keywords: insider threats, behavioral analytics, information security.

Е.В.Сероштан¹, А.С.Сивова²**РОЛЬ ТЕХНОЛОГИИ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ В ДЕТЕКЦИИ ИНСАЙДЕРСКИХ УГРОЗ В КОРПОРАТИВНОЙ СРЕДЕ**

В настоящем исследовании поведенческая аналитика рассматривается как мощный инструмент кибербезопасности. Представлены результаты теоретического исследования, раскрывающие роль технологии в выявлении инсайдерских угроз в корпоративной среде. Анализируются актуальные статистические данные, характеризующие динамику зарегистрированных утечек данных по вине внутренних нарушителей как в мире, так и в нашей стране. Выделены основные типы инсайдеров, обращено внимание на поведенческие индикаторы, показаны сильные и слабые стороны поведенческой аналитики, которые необходимо учитывать при её внедрении в практику российских организаций в контексте соблюдения нормативно-правовых норм действующего законодательства. Теоретическая и практическая ценность исследования заключается в обобщении актуальной информации и возможности её использования для повышения безопасности конфиденциальной информации от инсайдерских угроз.

Ключевые слова: инсайдерские угрозы, поведенческая аналитика, информационная безопасность.

DOI: 10.36807/2411-7269-2026-3-46-49-52

В современном мире компании всё чаще сталкиваются с проблемой утечек информации. И что интересно, далеко не всегда эти утечки происходят по вине внешних хакеров. Очень часто данные уносятся сами сотрудники – намеренно или случайно. Такие угрозы называют инсайдерскими, и они становятся настоящей угрозой для служб безопасности.

Проблема в том, что выявить инсайдера очень сложно. Хакер извне оставляет следы, когда взламывает систему, а сотрудник работает с данными легально – у него есть доступ, он может копировать файлы, отправлять письма. Антивирусы и стандартные системы защиты работают по принципу "нарушитель – тот, кто делает что-то запрещённое". Но если сотрудник делает разрешённые вещи, но в корыстных целях, техника этого "не видит".

Однако в последние годы появились технологии, которые могут помочь в решении этой проблемы. Речь идёт о поведенческой аналитике. Суть подхода в том, чтобы не ждать, когда сотрудник нарушит правило, а наблюдать за тем, как он обычно работает. Система запоминает, с какими файлами человек работает, в какое время приходит на работу, с кем общается. А потом – ищет отклонения. Если бухгалтер вдруг за пределами рабочего дня начинает скачивать чертежи, это повод задуматься.

¹ Сероштан Е.В., ассистент кафедры стратегического управления; Федеральное государственное бюджетное образовательное учреждение высшего образования "Белгородский государственный технологический университет им. В.Г. Шухова", г. Белгород

Seroshtan E.V., Assistant of the Department of Strategic Management; Federal State Budgetary Educational Institution of Higher Education "Belgorod State Technological University named after V.G. Shukhov", Belgorod
E-mail: Seroshtan-m@yandex.ru

² Сивова А.С., студентка 4 курса, специальность "Экономическая безопасность"; Федеральное государственное бюджетное образовательное учреждение высшего образования "Белгородский государственный технологический университет им. В.Г. Шухова", г. Белгород

Sivova A.S., 4th year Student, majoring in Economic Security; Federal State Budgetary Educational Institution of Higher Education "Belgorod State Technological University named after V.G. Shukhov", Belgorod
E-mail: sivova.arina@inbox.ru

Цель данной работы – рассмотреть, как поведенческая аналитика помогает выявлять инсайдерские угрозы в компаниях. В статье будет рассказано о том, как работают алгоритмы анализа поведения, и какие практические задачи это позволяет решать.

Рассмотрим понятие инсайдерских угроз. Инсайдерские угрозы – потенциальная угроза для организации, исходящая от лиц внутри самой организации, таких как сотрудники, бывшие сотрудники, подрядчики или деловые партнёры, обладающие внутренней информацией о мерах безопасности, данных и компьютерных системах организации. Такая угроза может включать мошенничество, хищение конфиденциальной или коммерческой ценной информации, интеллектуальной собственности либо саботаж компьютерных систем [1].

Динамика количества зарегистрированных утечек данных по вине внутренних нарушителей в России и в мире за 2022–2025 гг. показана на Рис. 1 [2].

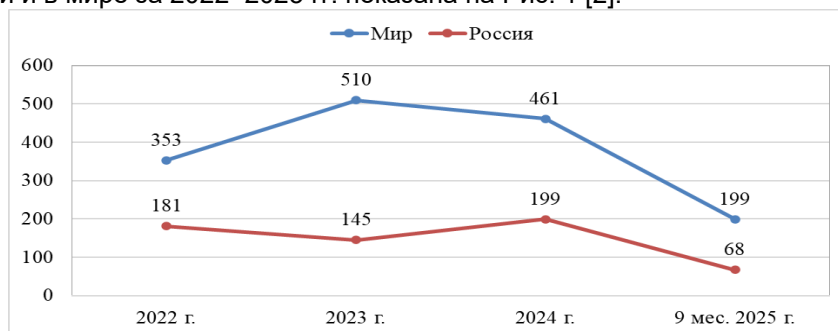


Рисунок 1 – Динамика количества зарегистрированных утечек данных по вине внутренних нарушителей в России и в мире, 2022–2025 гг.

Как видно из представленных на Рис. 1 данных, в 2025 г. большинство утечек данных в России, как и во всём мире носит умышленный характер. За весь период исследования (2022–2024 гг. и 9 мес. 2025 г.) было зарегистрировано случаев утечек по вине внутренних нарушителей: в мире – 1523, в нашей стране – 593. Самое большое количество случаев было зарегистрировано в мире в 2023 г. – более одной трети за весь анализируемый период (33,5%). В нашей стране аналогичная ситуация наблюдалась в 2024 г.: всего 199 случаев или 33,6%. В 2025 г. наметился вектор значительного снижения количества утечек данных по вине внутренних нарушителей в России, как и во всём мире [2].

Примерно треть всех утечек данных в банковской сфере происходит по вине собственных сотрудников. Это особенно опасно, так как работники имеют прямой доступ к секретной информации и понимают, как устроены внутренние процессы. Как следует из данных системного интегратора "Информзащита", по итогам за 9 мес. 2024 г. доля утечек информации из финансовых организаций, произошедших в результате действий инсайдеров (сотрудник, который имеет легальный доступ к информационным ресурсам компании), составила 31%. Этот показатель ниже, чем в аналогичном периоде 2023 г. (34%), но выше, чем в 2022 г. (28%) [3].

В результате анализа научных публикаций можно выделить следующие основные типы инсайдеров, для каждого из которых характерен собственный подход к их обнаружению [4]–[6].

1. Целенаправленные инсайдеры. Это сотрудники, которые действуют осознанно, обычно, это те, кто недоволен отношением к себе в компании или же работой руководителя. В данном случае могут быть разные мотивы, но обычно это желание заработать и(или) нанести убыток компании при увольнении. Данный тип инсайдера наиболее опасен, потому что действует скрытно и заранее готовится к утечке информации.

2. Халатность. Это самый распространённый тип инсайдеров. Они не хотят навредить компании, но при этом нарушают правила безопасности неосознанно или по невнимательности, что в итоге приводит к утечке информации. Например, работник берёт работу на дом на внешнем носителе, но не доходя до дома теряет её. В таком случае к данным компании могут получить доступ злоумышленники.

3. Скомпрометированные сотрудники. При этом вины сотрудника нет. Злоумышленники извне взломали компьютер работника и установили вредоносное программное обеспечение, с помощью которого могут иметь доступ к данным компании. Со стороны это выглядит так, как будто бы по вине сотрудника, выполняющего свои должностные обязанности, произошла утечка информации, однако на самом деле за этим стоит посторонний человек-злоумышленник.

Основная проблема инсайдеров в том, что их тяжело обнаружить. Со стороны всё выглядит легально – система видит просто работу сотрудника, однако за этим может скрываться опасность для организации. Исходя из вышеизложенного, традиционные методы защиты, которые ориентированы на блокировку угроз, имеющих источник извне, будут неэффективны. Требуется иной подход, который будет выявлять аномалии в поведении пользователя. Для этого используется поведенческая аналитика.

Поведенческая аналитика – это изучение данных, созданных действиями пользователей, обычно в цифровых средах, таких как веб-сайты, мобильные приложения или программные продукты. Также, поведенческую аналитику называют термином UEBA (User and Entity Behavior Analytics), что переводится как аналитика поведения пользователей и сущностей. В данном контексте под сущностью понимаются технические объекты: приложения, серверы и т.д. [7].

Концепция поведенческой аналитики заключается в том, чтобы построить цифровой профиль каждого сотрудника. В течение определённого периода система наблюдает за человеком и запоминает работу вне кризисных ситуаций. Информация собирается относительно всех работников, анализируется и выделяются усреднённые показатели по компании [8].

Для построения профиля система использует огромное количество информации из разных источников. При этом учитывается график работы; устройства и локации, используемые для работы; используемая документация; общение с коллегами; объём обычно передаваемых данных по электронной почте или через мессенджеры; скорость, с которой работник печатает и водит мышью.

После построения профиля система начинает сравнивать текущую работу с собранными данными "обычного поведения" сотрудника. Как только возникает отклонение – система фиксирует и повышает уровень подозрения. Важно понимать, что одно отклонение не указывает на инсайдерскую угрозу, необходима совокупность факторов. Например, если сотрудник задержался – это возможно не угроза, однако если же при этом начинает скачивать документы, с которыми до этого не работал – это уже цепочка событий, которая указывает на возможный риск. Рассмотрим другой сценарий. Если же это целенаправленная кража данных, то опытные инсайдеры понимают, что массовое копирование информации легко заметить, поэтому они действуют осторожно – скачивают её в малых количествах. По отдельности каждое такое действие безобидно, сложно увидеть возможную угрозу, однако в рамках поведенческой аналитики анализ осуществляется в динамике. Даже если каждый отдельный случай вписывается в политику безопасности, то общая картина уже указывает на проблему.

Безусловно, поведенческая аналитика (UEBA) – мощный инструмент кибербезопасности, однако, имеет свои сильные и слабые стороны. Рассмотрим сначала плюсы:

1. Поиск аномалий. UEBA находит то, что пропустят сигнатурные методы: необычное поведение пользователя, ранние признаки целевых атак или действия инсайдера.
2. Экономия времени. Система берёт на себя анализ поведения, освобождая специалистов от ручной работы.
3. Реагирование в реальном времени. Позволяет моментально отслеживать угрозу и принимать меры.
4. Расследование инцидентов. Помогает связывать разрозненные события в единую картину для поиска внутренних нарушителей.

К минусам относят:

1. Ложные срабатывания. На старте система может ошибочно реагировать на обычные изменения: отпуск сотрудника, смену задач или командировку. Без настройки это перегружает команду тревогами.
2. Сложность выводов. UEBA выдаёт не готовый диагноз ("вирус"), а процент отклонения от нормы. Чтобы понять результат, нужны специалисты, обладающие соответствующей квалификацией и умением грамотно интерпретировать полученные графики.
3. Зависимость от данных. Аналитика бесполезна без качественной телеметрии (HR-системы). Без контекста она либо пропустит угрозу, либо отреагирует на обычную активность.
4. Риск ошибок. Модели могут устаревать при изменении бизнес-процессов. Без понимания контекста система не способна отличить аврал на работе от подготовки к диверсии.

Когда речь заходит о наблюдении за сотрудниками, неизбежно возникают вопросы, выходящие за рамки технологий. Поведенческая аналитика, при всей её полезности для обеспечения безопасности, вторгается в сферу личного пространства человека.

Первое, с чем сталкивается компания, решившая внедрить поведенческую аналитику, – это необходимость соблюдать законодательство о защите персональных данных. В России действует Федеральный закон "О персональных данных" № 152-ФЗ. Он регулирует сбор, хранение и обработку персональных данных.

С точки зрения закона, данные о том, с какими файлами работает сотрудник, в какое время приходит на работу, с кем общается, – это персональные данные. А иногда и специальная категория персональных данных, если речь идёт, например, о биометрии или о данных, которые могут раскрывать личную жизнь.

Чтобы законно собирать такую информацию, компания обязана выполнить несколько условий. Во-первых, получить согласие сотрудника на обработку персональных данных. Во-

вторых, чётко определить цели сбора и не использовать данные для других целей. В-третьих, обеспечить защиту собранной информации от утечек и несанкционированного доступа.

На практике это означает, что установить данную систему, не поставив в известность работников, нельзя – это будет прямым нарушением закона.

Также, стоит отметить, что сложным является найти границу между рабочим пространством и личным. В рамках поведенческой аналитики формируется база данных, которая может включать как данные, характеризующие исполнение функциональных обязанностей, так и данные, характеризующие, например, личное общение в мессенджерах в период перерыва для отдыха и питания.

Компании решают эту проблему по-разному. Некоторые устанавливают жёсткие правила: запрет на использование рабочего устройства в личных целях. Другие, наоборот, сознательно ограничивают сбор данных, исключая из мониторинга определённые виды информации, например, заголовки писем в личной переписке. Третьи фокусируются лишь на выявленных в поведенческой аналитике аномалиях. При этом детальная информация, полученная в формате поведенческой аналитики, не подлежит анализу и не сохраняется.

Важно также отметить, что тотальный мониторинг оказывает влияние на паттерны поведения работников в процессе их взаимодействия в коллективе, на их реакцию на возникающие ситуации в профессиональной среде. Более того, у отдельных работников может возникнуть дискомфортное состояние в силу понимания того, что все его действия фиксируются и анализируются в рамках поведенческой аналитики. Одновременно, отдельные сферы деятельности, требующие специальных условий для обеспечения кибербезопасности, например, оборонно-промышленный комплекс, финансово-кредитная система, обуславливают внедрение поведенческой аналитики. Это находит отражение в соответствующих локальных нормативно-правовых документах, о чём обязательно информируют работников, которые спокойно воспринимают методы поведенческой аналитики.

Таким образом, поведенческая аналитика является мощным инструментом кибербезопасности, однако, имеет свои сильные и слабые стороны, что необходимо учитывать при внедрении этой технологии.

Список использованных источников

1. Ивлиева Н.А. Инсайдерские риски как угроза корпоративным информационным системам / Н.А. Ивлиева // Экономика и предпринимательство. – 2025. – № 7(180). – С. 1056-1059.
2. Утечки данных вследствие действий внутренних нарушителей. Мир – Россия, 2022–2025 гг. – URL: <https://www.infowatch.ru/> (дата обращения: 30.04.2026).
3. Финансовые организации теряют данные из-за действий собственных сотрудников. – URL: <https://www.kommersant.ru/doc/7281929> (дата обращения: 30.04.2026).
4. Исаков Р.О., Шапошников А.Ю. Инсайдерская информация как угроза информационной безопасности: понятие, информационная и правовая природа // Вестник молодых учёных и специалистов Самарского университета. – 2025. – № 3(28). – С. 84-92.
5. Шугаев В.А. Классификация инсайдерских угроз информации / В.А. Шугаев, С.П. Алексеенко // Вестник Воронежского института МВД России. – 2020. – № 2. – С. 143-153.
6. Селезнева Е.Ю. Система предотвращения инсайдерских угроз и утечки ключевой информации в условиях гибридного формата работы / Е.Ю. Селезнева, В.Р. Рыжкова, Н.А. Рыжкова // Вектор экономики. – 2025. – № 12(114).
7. Поведенческая аналитика (Behavioral Analytics) // FoxData: [глоссарий]. – URL: <https://foxdata.com/ru/glossary/behavioral-analytics/> (дата обращения: 30.04.2026).
8. Метелкин П.А. Архитектура системы мониторинга инсайдерских угроз с гарантией конфиденциальности на основе Privacy by Design / П.А. Метелкин // Вестник науки. – 2026. – Т. 2. – № 1(94). – С. 552-559.