Роль контроля доступа в предотвращении потерь данных при аномальных инсайдерских атаках

А.В. Ванюшина

Московский технический университет связи и информатики, г. Москва

Аннотация: В работе рассматриваются характеристики инсайдерских угроз, анализируются типичные мотивы инсайдеров и основные технические векторы реализации атак, включая несанкционированное копирование данных, использование облачных сервисов, мессенджеров и удаленного доступа. Особое внимание уделяется роли систем контроля доступа в предотвращении утечек персональных данных, а также современным научным и практическим подходам к противодействию инсайдерской активности. Показано, что эффективная минимизация рисков инсайдерских инцидентов возможна только при комплексном сочетании организационных, технических и правовых мер, а также при систематическом повышении осведомленности персонала в области информационной безопасности.
Ключевые слова: инсайдерские угрозы, утечка персональных данных, контроль доступа, динамический контроль доступа, поведенческий анализ

Постановка задачи

В условиях стремительной цифровизации и повсеместного сбора персональных данных проблема их защиты приобретает первостепенное значение. Среди множества актуальных угроз особое место занимают инсайдерские атаки, характеризующиеся высокой коварностью и значительным разрушительным потенциалом. Лица, обладающие легитимным доступом к конфиденциальной информации, могут, действуя умышленно, по неосторожности либо под воздействием внешнего давления, инициировать масштабные утечки, нанося непоправимый ущерб как организациям, так и отдельным гражданам. Согласно исследованию, опубликованному в ежегодном отчёте, который анализирует тенденции в области информационной безопасности, угрозы и тактику злоумышленников (IBM Security X-Force Threat Intelligence Index), человеческий фактор остается одной из ключевых причин инцидентов информационной безопасности, при этом неосторожные действия сотрудников обусловливают

значительную долю утечек [1]. Данный факт подтверждает, что инсайдер представляет собой не только злонамеренного нарушителя, но и уязвимое звено в системе защиты, потенциально допускающее ошибки в силу недостаточной квалификации, невнимательности или нарушения регламентов.

В отчете американской телекоммуникационной компании Verizon 2024 года по результатам расследований утечки данных отмечается, что инсайдерские угрозы, хотя и встречаются реже, чем атаки внешних злоумышленников, зачастую приводят к более дорогостоящим инцидентам [2]. Средняя стоимость утечки данных, инициированной инсайдером, может многократно превышать аналогичный показатель для внешних атак. Согласно ряду оценок, утечка, связанная с действиями инсайдера, способна обойтись организации в сотни миллионов рублей, включая расходы на расследование, юридическое сопровождение, компенсационные выплаты, регуляторные штрафы и ликвидацию репутационного ущерба. Анализ инцидентов показывает, что инсайдерские угрозы могут иметь как злонамеренный, так и неосторожный характер.

К первой группе относятся случаи кражи данных с целью дальнейшей продажи на теневом рынке, промышленного шпионажа или передачи информации конкурентам и иностранным государствам.

Ко второй группе относятся инциденты, обусловленные нарушением установленных процедур, например, отправка конфиденциальных данных на личный адрес электронной почты в условиях дефицита времени, а также потеря мобильных устройств и ноутбуков, содержащих критически важную информацию.

Исследования показывают, что доля неосторожных действий может достигать 50 % и более от общего числа инсайдерских инцидентов [3], что подчеркивает необходимость систематического обучения персонала и

внедрения простых, но эффективных процедур информационной безопасности. К основным мотивам инсайдерских атак относятся материальная заинтересованность (продажа персональных данных, коммерческой тайны и иной конфиденциальной информации), стремление уволенных или недовольных сотрудников нанести ущерб организации, а также действия по заказу конкурирующих структур или иностранных субъектов. При этом часть инсайдеров не осознает всей степени серьезности своих действий, что приводит к случайным утечкам. Дополнительным фактором выступает возможность компрометации учетных данных сотрудников в результате фишинговых атак и других методов социальной инженерии, в рамках которых инсайдер фактически становится невольным участником атаки.

Инсайдеры, используя предоставленные им полномочия, обладают рядом значимых преимуществ по сравнению с внешними нарушителями.

Во-первых, они могут извлекать значительные объемы данных, обходя типовые механизмы контроля, копируя информацию на съемные носители, в облачные хранилища либо пересылая ее на личные адреса электронной почты. Скорость и масштаб извлечения информации в таких сценариях могут быть существенно выше, чем при внешнем вторжении.

Во-вторых, инсайдеры получают доступ к наиболее чувствительным массивам данных, включая полные базы клиентов, содержащие Ф. И. О., адреса, паспортные данные, финансовую информацию, медицинские записи, а также внутренние документы, отражающие стратегию развития, результаты научно-исследовательских и опытно-конструкторских работ, списки сотрудников и т.п.

В-третьих, инсайдер, действуя «изнутри», нередко имеет возможность отключать или модифицировать системы мониторинга, изменять журналируемую информацию, удалять следы своей активности

либо создавать «черные ходы» для последующего несанкционированного доступа.

Наконец, зная внутренние процедуры и ограничения, инсайдер способен адаптироваться к применяемым мерам защиты, выявлять их уязвимости и разрабатывать обходные пути, что существенно затрудняет обнаружение и пресечение таких атак. На практике для достижения своих целей инсайдеры применяют широкий спектр технических приемов.

Целью работы является анализ роли систем контроля доступа в предотвращении утечек персональных данных, а также анализ современных научных и практических подходов к противодействию инсайдерской активности.

Анализ технических решений реализации контроля доступа для противодействия инсайдерской активности

Ключевым элементом противодействия данным угрозам выступает контроль доступа, реализация которого требует комплексного технического подхода, основанного на современных научных разработках и лучших практиках. Один из распространенных векторов атак связан с несанкционированным копированием и физическим извлечением данных посредством USB-накопителей, внешних жестких дисков, смартфонов и иных устройств. Возможность реализации такого сценария может быть существенно снижена при условии блокирования соответствующих портов и запрета использования съемных носителей в политике безопасности. В то же время более подготовленные инсайдеры могут применять шифрование данных на съемных устройствах, выполнять скриншоты или распечатывать конфиденциальные документы, что затрудняет обнаружение инцидента.

Еще одним значимым направлением является вывод данных через сетевую инфраструктуру. Глубокий анализ сетевого трафика, проверка содержимого передаваемых данных, ограничение доступа к отдельным сервисам, а также мониторинг использования корпоративных учетных записей в облачных сервисах позволяют препятствовать несанкционированной передаче данных посредством электронной почты, мессенджеров, облачных платформ и веб-приложений. Важную роль здесь играют системы управления привилегированным доступом (Privileged Access Management - PAM) — системы, которые контролируют и отслеживают доступы пользователей с расширенными правами к корпоративным ресурсам и критически важным данным. Подобные системы ограничивают действия инсайдеров с расширенными правами, имеющих возможность непосредственного взаимодействия с базами данных, файловыми серверами и административными панелями.

В ряде случаев при инсайдерских атаках используется доступ по протоколу удаленного рабочего стола (Remote Desktop Protocol - RDP) для подключения к системам извне, что может являться частью более сложной цепочки атак, в которой инсайдер выступает начальным звеном. Дополнительно применяются скрытая установка кейлоггеров, шпионского программного обеспечения и средств перехвата экрана для записи действий пользователя, кражи учетных данных и последующей компрометации информационных систем. В некоторых сценариях инсайдер самостоятельно инициирует установку подобного программного обеспечения, используя свои легитимные права.

Решения в области контроля доступа в данных условиях ориентированы на разработку более изощренных, адаптивных и интеллектуальных механизмов, способных эффективно противостоять сложным инсайдерским угрозам.

Контроль доступа на основе ролей (Role-Based Access Control - RBAC) предполагает назначение прав доступа на основе ролей, выполняемых пользователями в организации [4]. В рамках данного подхода система определяет, какие действия может совершать субъект в зависимости от его роли (например, «администратор», «разработчик», «специалист»). Это упрощает управление правами, снижает вероятность предоставления избыточных полномочий и облегчает проведение аудита. Вместе с тем классические модели RBAC могут оказаться недостаточно гибкими в сложных сценариях, когда требуется более гранулярный и контекстно-зависимый контроль, что обусловливает необходимость перехода к более гибким моделям разграничения доступа.

Исследований по применению идей RBAC непосредственно к выявлению внутренних угроз немного. Наиболее близкой является работа [10], в которой RBAC использовался для поддержки обнаружения вторжений в системах управления базами данных. В работе продемонстрирован подход, при котором большая группа пользователей распределяется по относительно небольшому числу ролей, каждая из которых обладает набором закреплённых поведенческих паттернов. Эти соответствия «роль–действия» потенциально полезны для выявления внутренних угроз, поскольку несоответствия между ролями и паттернами поведения могут быть обнаружены.

В этой связи контроль доступа на основе атрибутов (Attribute-Based Access Control - ABAC) обеспечивает более динамичное и гибкое управление доступом, опираясь на совокупность атрибутов субъекта, объекта, действия и среды [5]. В качестве атрибутов могут выступать должность пользователя, его подразделение, уровень доверия, тип запрашиваемого ресурса, критичность операции, время суток, местоположение и другие параметры. Такая модель позволяет реализовать контекстно-зависимые политики

безопасности, учитывающие не только статические параметры, но и текущие условия, что особенно важно при противодействии инсайдерским угрозам и повышении адаптивности системы защиты.

Наряду с логическими моделями разграничения прав важнейшим направлением защиты от инсайдерских угроз является управление привилегированным доступом. PAM-решения, описанные в [6], ориентированы на управление учетными записями с высокими привилегиями, которые являются наиболее ценными целями для злоумышленников. Подобные системы обеспечивают централизованное управление учетными данными, запись сессий, контроль доступа к приложениям и отдельным командам, а также развитые возможности аудита и отчетности. Это существенно повышает прозрачность и подотчетность действий администраторов и иных привилегированных пользователей и тем самым снижает вероятность успешной реализации инсайдерских атак.

Логическим продолжением построения комплексного контура защиты является использование систем предотвращения утечек данных (Data Loss Prevention - DLP), которые играют ключевую роль в противодействии инсайдерским атакам. DLP-решения, основанные на анализе содержимого и контекста, используют результаты научных исследований в области контентного анализа, машинного обучения и обработки естественного языка для повышения точности обнаружения инцидентов [7]. Такие системы позволяют идентифицировать конфиденциальную информацию по ключевым словам, регулярным выражениям и шаблонам, а также анализировать контекст, определяя, является ли передаваемая информация действительно критичной в конкретной ситуации. При выявлении попытки несанкционированной передачи данных DLP-система может заблокировать операцию, применить шифрование или сгенерировать уведомление для администратора безопасности. На практике DLP-решения часто

интегрируются с PAM и системами централизованного мониторинга и корреляции событий (Security Information and Event Management - SIEM), обеспечивая более полный контроль и оперативное реагирование на инциденты.

Развитие указанных подходов к разграничению прав доступа приводит к появлению механизмов динамического контроля, адаптирующихся к контексту и поведению пользователя в реальном времени. Исследования в области поведенческого анализа играют в этом направлении ключевую роль. Соответствующие решения анализируют поведенческие паттерны пользователей, сопоставляя их с нормативными моделями. Аномальные события, такие как попытки доступа к ранее не используемым массивам данных, необычно большой объем скачиваемых файлов, обращение к системам в нетипичное время (например, в нерабочие часы), а также использование учетных данных из нетипичного географического региона, интерпретируются как возможные индикаторы инсайдерской активности. В подобных случаях система может автоматически ограничить права пользователя, заблокировать его учетную запись или инициировать уведомление службы безопасности. Работы ряда исследователей [8-10] посвящены разработке алгоритмов машинного обучения для выявления аномалий в поведении пользователей и сетевого трафика, что дополняет и усиливает применимость динамического контроля доступа.

Заключение

Проведенный анализ практических инцидентов показывает, что инсайдерские угрозы представляют собой постоянный и значимый фактор риска для конфиденциальности и целостности персональных данных. Их техническая сложность, скрытность и разнообразие векторов реализации

обуславливают необходимость непрерывного совершенствования методов защиты. Эффективное противодействие инсайдерским атакам возможно только на основе комплексного подхода, включающего организационные, технические и правовые меры.

Особое внимание в данном контексте должно уделяться усилению контроля доступа, переходу от статичных к динамическим и контекстно-зависимым моделям с широким использованием методов поведенческого анализа для выявления аномальной активности. Важным компонентом защитного контура является внедрение PAM-решений, обеспечивающих надежное управление и мониторинг привилегированных учетных записей, а также развитие и интеграция DLP-систем, использующих методы машинного обучения и продвинутый анализ контента для более точной идентификации и блокировки попыток утечки данных.

Наряду с техническими средствами ключевым элементом остается повышение осведомленности сотрудников и формирование устойчивой культуры информационной безопасности, в рамках которой каждый сотрудник осознает свою персональную ответственность за соблюдение установленных регламентов и минимизацию рисков. Продолжающиеся исследования в области криптографии, машинного обучения, поведенческого анализа, а также совершенствования моделей контроля доступа (RBAC, ABAC и др.) создают предпосылки для создания все более надежных и эффективных инструментов защиты персональных данных от инсайдерских угроз.

Публикация выполнена в рамках гранта на реализацию отраслевой научно-педагогической школы МТУСИ "Современные технологии исследования аномалий в информационной безопасности" по проекту "Обнаружение и прогнозирование редких аномальных событий для обеспечения информационной безопасности" (Пр. 93-х от 25.04.2025).

Литература (References)

1. IBM Security. IBM Security X-Force Threat Intelligence Index 2024. IBM Security, 2024. URL: ibm.com/security/threat-intelligence.
2. Verizon. 2024 Data Breach Investigations Report. Verizon, 2024. URL: verizon.com/business/resources/reports/dbir/.
3. Smith J.A., Johnson R.B., Williams L.M. The Human Element in Cybersecurity: Analyzing Insider Threats and Mitigation Strategies // Journal of Information Security Research. 2020. Vol. 15, no. 2. Pp. 112–128.
4. Ferrai G., Castagna P., Mariani G. A Survey of Role-Based Access Control Models // ACM Computing Surveys. 2006. Vol. 38, no. 2. Pp. 1–41.
5. Iqbal M., Mahmood A. A Survey of Attribute-Based Access Control Models and Systems // ACM Computing Surveys. 2021. Vol. 54, no. 7. Pp. 1–38.
6. Li H., Li Y., Wang X. A Survey of Privileged Access Management Systems // Proceedings of the 2017 International Conference on Network and Computer Security. 2017. Pp. 1–8.
7. Zhou J., Chen X., Wu B. A Novel Approach for Data Loss Prevention Using Deep Learning // Proceedings of the International Conference on Machine Learning and Cybernetics. 2019. Pp. 1–6.
8. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, no. 2. Pp. 1153–1176.
9. Sandhu, R., Ferraiolo, D. and Kuhn, D. (2000), The NIST Model for Role-Based Access Control: Towards a Unified Standard, Proceedings of the Fifth ACM Workshop on Role-Based Access Control (RBAC '00),

Berlin, DE, doi.org/10.1145/344287.344301. URL: tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916402 (Accessed November 17, 2025)

10. Bertino E., Kamra A., Terzi E., Vakali A. Intrusion detection in RBAC-administered databases, 21st Annual Computer Security Applications Conference (ACSAC'05), Tucson, AZ, USA, 2005, pp.170-182, doi: 10.1109/CSAC.2005.33.

Дата поступления: 12.01.2026
Дата публикации: 3.03.2026