УДК 338.264 DOI: 10.14451/1.251.221

Обеспечение безопасности данных при внедрении аналитических платформ в корпоративной среде

© 2025 **Шнайдер Виктор Викторович**
Кандидат экономических наук, доцент. Финансовый университет при Правительстве РФ, Москва.
E-mail: vvshnajder@fa.ru

Ключевые слова: аналитические платформы, безопасность данных, угрозы информационной безопасности, управление рисками, системы контроля доступа, шифрование данных, мониторинг инцидентов, корпоративная архитектура.

В данной статье рассматривается комплексный анализ угроз безопасности данных в современных аналитических платформах, превратившихся из инструментов генерации отчетов в стратегически важные компоненты корпоративной архитектуры. Исследуется многомерная классификация платформ, функциональный ландшафт решений и архитектурная сложность, создающая уязвимые места вследствие централизованного хранения корпоративных данных. Детально анализируются диверсифицированные векторы атак, включая внешние угрозы, компрометацию цепочек поставок и внутренние риски, связанные с действиями инсайдеров и ошибочными конфигурациями систем. Предлагается многоуровневая система защиты, основанная на принципе эшелонированной обороны, сочетающая превентивные, детективные и корректирующие меры, архитектурные решения сегментации безопасности, современные механизмы контроля доступа, сквозное шифрование данных, а также комплексные подходы к мониторингу и реагированию на инциденты.

Введение

В условиях стремительной цифровизации экономики и перехода к модели управления, основанной на данных, корпорации сталкиваются с парадоксальной ситуацией, когда инструменты, призванные повышать эффективность, одновременно создают беспрецедентные угрозы для конфиденциальности и целостности критически важной бизнес-информации, что превращает задачу обеспечения безопасности в один из ключевых факторов устойчивого развития организации.

Бизнес-аналитика, преодолевшая стадию простого ретроспективного описания произошедших событий, представляет собой целостную методологию, охватывающую полный цикл работы с корпоративными данными — от их сбора и очистки до сложного статистического моделирования и визуализации результатов. Описательный анализ служит фундаментом, систематизируя исторические данные в интуитивно понятные дашборды, диагностический анализ углубляется в установление причинно-следственных связей через методы корреляционного и регрессионного анализа, тогда как

предсказательный анализ, опираясь на алгоритмы машинного обучения, строит вероятностные сценарии развития бизнес-процессов. Завершает эту цепь предписывающая аналитика, которая не только прогнозирует возможные исходы, но и рекомендует конкретные управленческие действия, оптимизируя таким образом ключевые показатели эффективности организации в условиях неопределенности рыночной среды.

Основу исследования составили работы таких авторов, как Walha, A., Ghozzi, F. и др. [10], Cecil R. R., Soares J. [8], Haik N., Jenkins P. и др. [7], Димитриади Г. Д. [2], Бариленко В. И., Никифорова Е. В., Музалев С. В. [1], Толмачев М. Н. [3–5] и пр.

Цель исследования

Целью данной работы является комплексный анализ угроз безопасности данных в современных аналитических платформах и разработка многоуровневой системы защиты.

Методы исследования

В рамках данного исследования были применены методы системного анализа, количественной оценки рисков и сравнительного анализа архитектурных решений корпораций.

Результаты исследования и их обсуждение

Современные аналитические платформы, превратившиеся из инструментов генерации отчетов в стратегически важные компоненты корпоративной архитектуры, функционируют как цифровые командные центры, которые в реальном времени аккумулируют эксабайты структурированных и неструктурированных данных из различных источников. Такие источники включают в себя транзакционные базы данных, потоки телеметрии с промышленного оборудования, ленты социальных сетей и даже открытые государственные реестры, обеспечивая сквозную аналитику всего жизненного цикла продукции или услуги. Стоит отметить, что при этом их интеграция с системами планирования ресурсов предприятия и управления взаимоотношениями с клиентами создает единое информационное пространство, где перекрестный анализ финансовых, операционных и поведенческих метрик выявляет ранее скрытые зависимости, а встроенные модули искусственного интеллекта автоматизируют процессы кластеризации, классификации и прогнозирования. Однако такая всеобъемлющая связность и глубина проникновения в бизнес-процессы создает уязвимые места, поскольку централизованное хранение и обработка корпоративного банка данных формирует критическую точку отказа, привлекательную как для внешних угроз, так и для внутренних, которые способны нанести непоправимый ущерб репутации и конкурентоспособности компании.

Классификация аналитических платформ представляет собой многомерную матрицу, где системы дифференцируются по технологическому стеку, глубине аналитического охвата, целевой аудитории и методологии обработки данных. Базовое разделение проходит между традиционными BI-системами, ориентированными на бизнес-пользователей и предоставляющими интуитивные инструменты визуализации и самообслуживания, и платформами для работы с большими данными, требующими продвинутых компетенций в области Data Science и инженерии данных.

«Функциональный ландшафт современных аналитических решений охватывает полный цикл работы с данными, начиная с этапа интеграции и консолидации разрозненных источников через ETL/ELT-процессы, где системы демонстрируют способность к подключению как к реляционным базам данных и корпоративным хранилищам, так и к облачным объектным хранилищам, API внешних сервисов и потокам IoT-устройств» [10].

«Среди популярных решений доминируют как универсальные платформы-лидеры рынка, так и узкоспециализированные инструменты. Стоит отметить, что отдельную нишу занимают комплексные платформы типа IBM Watson Studio, сочетающие возможности традиционной бизнес-аналитики с продвинутыми AI-функционалами, включая компьютерное зрение и обработку естественного языка, что позволяет корпорациям создавать сквозные аналитические цепочки

от сбора сырых данных до генерации автоматизированных управленческих рекомендаций» [8].

Современные программные решения в сфере бизнес-аналитики:

- Tableau.
  Передовая технология визуального исследования данных через естественно-интуитивный интерфейс, позволяющий строить сложные интерактивные дашборды без написания кода.
- Power BI от Microsoft.
  Выигрывает за счет глубокой интеграции с экосистемой Office 365 и Azure, предлагая корпорациям единую среду для совместной работы с данными.
- Qlik Sense.
  Примечательна ассоциативной аналитической технологией, выявляющей скрытые связи across всего массива информации.
- Hadoop-экосистема.
  Лидирует в области Big Data с ее распределенной файловой системой HDFS и фреймворком MapReduce для пакетной обработки огромных объемов данных.
- Apache Spark.
  Обеспечивает возможность потоковой обработки и встроенные библиотеки машинного обучения MLlib.
- Облачные платформы типа Google BigQuery и Amazon Redshift.
  Предоставляют managed-сервисы для анализа петабайтных массивов с использованием архитектуры MPP.

Проблематика безопасности данных в аналитических платформах формирует комплекс взаимосвязанных вызовов, которые исходят из фундаментального противоречия между необходимостью обеспечения свободного доступа к данным для аналитиков и требованием их строгой защиты, где каждая дополнительная интеграция с новыми источниками данных или бизнес-приложениями расширяет периметр безопасности и создает потенциальные векторы для компрометации информации. Архитектурная сложность современных аналитических решений, сочетающих облачные и локальные компоненты, многоуровневые хранилища и разнородные протоколы обмена, значительно усложняет задачу унифицированного применения политик безопасности и соблюдения регуляторных требований в условиях постоянно эволюционирующих киберугроз.

Основные угрозы безопасности данных в аналитических платформах проявляются через:

- диверсифицированные векторы атак, где внешние угрозы включают целенаправленные кампании по эксплуатации уязвимостей в веб-интерфейсах;
- атаки на цепочки поставок программного обеспечения через компрометацию сторонних библиотек;
- сложные социально-инженерные атаки на сотрудников с привилегированным доступом;

К внутренним угрозам можно отнести:

- умышленные действия инсайдеров, злоупотребляющих своими полномочиями для несанкционированного копирования или модификации данных, так и непреднамеренные нарушения, вызванные недостаточной компетенцией персонала в вопросах кибербезопасности;
- ошибочные конфигурации систем, где особую опасность представляют комбинированные атаки, когда внешний злоумышленник сначала получает доступ через компрометированного сотрудника, а затем использует его легитимные привилегии для горизонтального перемещения по аналитической платформе.

Особенности работы с большими объемами и разнородностью данных создают уникальные операционные риски, поскольку распределенные архитектуры обработки, основанные на принципах горизонтального масштабирования, требуют применения специализированных механизмов безопасности, способных функционировать в условиях постоянной миграции данных между вычислительными узлами и хранилищами различного типа. Разнородность форматов затрудняет единообразное применение политик

классификации и защиты, тем самым вынуждая организации внедрять сложные системы автоматического распознавания контекста данных и динамического применения мер безопасности в зависимости от типа контента, его чувствительности и текущего местоположения в аналитическом конвейере.

Анализ уязвимостей и рисков при внедрении аналитических платформ требует системного подхода, учитывающего как технические аспекты интеграции новых систем в существующую ИТ-инфраструктуру, так и организационные изменения бизнес-процессов. Каждая стадия внедрения, от первоначального развертывания до полной интеграции с корпоративными системами, порождает уникальные векторы атак и точки уязвимости, требующие проведения тщательной оценки в контексте конкретной архитектуры и модели использования платформы.

«Критически важным представляется проведение предварительного моделирования угроз с использованием методологий типа STRIDE или PASTA, которые позволяют выявить потенциальные уязвимости на ранних этапах проектирования архитектуры» [7]. Стоимость внесения изменений в систему безопасности минимальна, при этом особое внимание уделяется анализу точек интеграции с унаследованными системами и внешними сервисами, где чаще всего возникают проблемы совместимости протоколов и разрыв в уровнях безопасности между различными компонентами корпоративной ИТ-среды.

На технологическом уровне ключевые риски связаны с неправильной конфигурацией компонентов платформы, особенно в распределенных средах обработки данных, где несоблюдение принципа минимальных привилегий при настройке прав доступа к кластерам Hadoop или Spark может привести к несанкционированному доступу к критически важным наборам информации. Отдельную категорию составляют риски, связанные с использованием открытых компонентов и библиотек в аналитических платформах, которые могут содержать известные уязвимости, не выявленные в процессе принятия решения. Особую сложность представляет поддержание актуальности версий программного обеспечения в условиях непрерывной разработки и обновления функциональности платформы, когда новые функции могут привносить непредусмотренные уязвимости в уже работающую систему. Организационные риски внедрения проявляются в недостаточном уровне осведомленности пользователей о правилах работы с аналитическими платформами, что приводит к непреднамеренным нарушениям политик безопасности (от размещения конфиденциальных отчетов в общедоступных рабочих областях до использования слабых учетных данных для доступа к чувствительным данным). При этом отсутствие четких процедур управления жизненным циклом учетных записей создает риск накопления избыточных привилегий у сотрудников, меняющих должностные обязанности или покидающих организацию. Существенным вызовом является обеспечение соответствия регуляторным требованиям при обработке персональных данных в аналитических платформах, где сложность представляет реализация прав субъектов данных на удаление или исправление информации в условиях распределенных систем хранения и сложных цепочек обработки.

«Для комплексной оценки рисков рекомендуется применять количественные методы анализа, включая расчет показателей ALE (Annual Loss Expectancy) и ROSI (Return on Security Investment), которые позволяют обосновать необходимость внедрения конкретных мер защиты через оценку потенциального финансового ущерба от реализации угроз и эффективности затрат на безопасность» [9]. Особое значение приобретает создание системы непрерывного мониторинга уязвимостей, интегрированной с процессами управления изменениями в аналитической платформе, что обеспечивает своевременное выявление новых рисков по мере развития системы и изменения бизнес-требований.

Методы и подходы к обеспечению безопасности данных в аналитических платформах формируют многоуровневую систему защиты, основанную

на принципе эшелонированной обороны, где сочетаются превентивные, детективные и корректирующие меры. Дополнительным стратегическим подходом выступает реализация защиты данных на основе их классификации, когда для различных категорий информации применяются дифференцированные политики безопасности, включая автоматическое назначение меток конфиденциальности средствами машинного обучения, обеспечивающее пропорциональный уровень защиты без избыточного ограничения функциональности аналитических процессов.

Архитектурные решения и моделирование угроз при проектировании защищенных аналитических платформ требуют применения системного подхода, основанного на глубоком анализе бизнес-процессов и потенциальных векторов атак, где ключевым инструментом выступает создание формализованных моделей угроз с использованием методологии STRIDE. Такая методология позволяет идентифицировать риски спуфинга, несанкционированного изменения данных, отказа в обслуживании и эскалации привилегий на уровне отдельных компонентов системы.

Для комплексных распределенных архитектур рекомендуется применение методологии DFD (Data Flow Diagram) с последующим сопоставлением потоков данных с таксономией угроз, что обеспечивает визуализацию уязвимых точек интеграции между модулями платформы. С архитектурной точки зрения эффективной практикой является реализация принципа сегментации безопасности через создание изолированных сред обработки для данных различной категории конфиденциальности с использованием технологий микросервисов и контейнеризации, где каждый сервис обладает минимально необходимыми привилегиями и взаимодействует через защищенные API-шлюзы с обязательной аутентификацией и авторизацией каждого запроса.

В свою очередь «для защиты периметра отдельных компонентов применяются веб-применения-брандмауэры (WAF) и системы предотвращения вторжений (IPS), настроенные на специфичные для аналитических платформ паттерны атак, такие как инъекции в запросы к OLAP-кубам или манипуляции с параметрами визуализации» [2].

Средства контроля доступа и разграничения прав пользователей в современных аналитических платформах эволюционировали от простых систем ролевого управления доступом (RBAC) к гибридным моделям, сочетающим атрибутивный контроль доступа (ABAC) и мандатные механизмы защиты, где решения о предоставлении прав принимаются на основе динамического контекста (от должностныех обязанностей пользователя до географического местоположения, используемого устройства, время запроса и чувствительность запрашиваемых данных). Практической реализацией такого подхода выступают системы динамического управления доступом, которые в реальном времени оценивают уровень риска каждой операции. Например, попытка доступа к финансовым отчетам с неподключенного к корпоративной сети устройства может потребовать дополнительной аутентификации или полностью блокировать подозрительное действие.

Для административных функций платформы обязательным является внедрение принципа разделения привилегий (Privilege Separation) и Just-in-Time доступ, когда временные права предоставляются исключительно на период выполнения конкретной задачи с обязательным логированием всех действий привилегированных пользователей. Шифрование данных и управление ключами в контексте аналитических платформ требуют реализации сквозной криптографической защиты, охватывающей все состояния информации, где для защиты данных в состоянии покоя применяются блочные алгоритмы шифрования, обеспечивающие как конфиденциальность, так и целостность за счет использования аутентифицированных режимов работы.

Мониторинг, аудит и реагирование на инциденты в аналитических платформах образуют непрерывный цикл управления безопасностью, где системы мониторинга собирают телеметрию со всех компонентов платформы — от логов

аутентификации и запросов к базам данных до метрик использования вычислительных ресурсов и сетевого трафика; при этом применяются корреляция событий и поведенческий анализ для выявления аномалий. Для обеспечения полноценного аудита безопасности внедряются системы управления информацией и событиями безопасности (SIEM), агрегирующие данные из разнородных источников и позволяющие отслеживать соблюдение политик безопасности в режиме реального времени. На особом контроле находятся мониторинг действий привилегированных пользователей и отслеживание изменений в конфигурации критически важных компонентов платформы.

«Процесс реагирования на инциденты формализуется через создание планов действий для различных сценариев угроз, где современные организации все чаще внедряют платформы оркестрации, автоматизации и реагирования (SOAR). Такие платформы позволяют автоматизировать рутинные операции по блокировке подозрительных IP-адресов, отзыву скомпрометированных учетных записей и изоляции пораженных компонентов системы. Обязательным элементом является проведение регулярных учений по отработке действий при киберинцидентах с моделированием реальных атак на аналитическую платформу» [6].

Выводы

В заключение следует отметить, что эволюция аналитических платформ в стратегические компоненты корпоративной архитектуры сопровождается формированием сложного комплекса угроз безопасности, требующего системного подхода к защите данных. Проведенное исследование позволило выявить, что ключевыми результатами анализа современных решений являются: переход от традиционных BI-систем к гибридным платформам, интегрирующим возможности бизнес-аналитики с продвинутыми функциями искусственного интеллекта; систематизация угроз безопасности через призму архитектурной сложности платформ, где выделяются внешние векторы атак, включающие эксплуатацию уязвимостей веб-интерфейсов и компрометацию цепочек поставок ПО, а также внутренние риски, связанные с действиями инсайдеров и ошибочными конфигурациями; разработка многоуровневой модели защиты, основанной на принципах эшелонированной обороны, сочетающей превентивные, детективные и корректирующие меры, где особое значение приобретают архитектурные решения в виде сегментированных сред обработки данных и внедрение динамических систем контроля доступа, оценивающих уровень риска операций в реальном времени.

Доказана эффективность применения методологий моделирования угроз STRIDE и DFD для идентификации уязвимостей на этапе проектирования, а также необходимость реализации сквозного шифрования данных с использованием перспективных технологий гомоморфного шифрования и конфиденциальных вычислений. Установлено, что организационные аспекты безопасности требуют формализации процессов управления жизненным циклом учетных записей и внедрения систем непрерывного мониторинга, интегрированных с платформами SOAR для автоматизации реагирования на инциденты. Полученные результаты формируют методологическую основу для разработки комплексных стратегий защиты аналитических платформ, обеспечивающих баланс между доступностью данных и требованиями безопасности в условиях динамично развивающейся киберугроз.

Библиографический список

1. *Бариленко В. И.*, *Никифорова Е. В.*, *Музалев С. В.* Аналитическое обоснование поддержки развития приоритетных отраслей российской экономики // РИСК: Ресурсы, Информация, Снабжение, Конкуренция. — 2022. — № 2. — С. 27—37.
2. *Димитриади Г. Д.* Основные методологии и подходы к моделированию бизнес-процессов компании // Символ науки. — 2023. — № 11-2—1. — С. 53—56.
3. *Петров А. М.* Раскрытие информации о социальных обязательствах в отчетности экономических субъектов // Экономические науки. — 2024. — № 231. — С. 182—185.

4. *Ряховская А. Н.*, *Мельник М. В.* Роль и организация внутреннего контроля за экономической устойчивостью хозяйствующих субъектов // Учет. Анализ. Аудит. — 2024. — Т. 11, № 5. — С. 69—78.
5. *Толмачев М. Н.* Ретроспективный статистический анализ развития строительной отрасли России // Экономические науки. — 2024. — № 230. — С. 185—189.
6. *Цымбал Ф. А.* Управление инцидентами безопасности и событиями (SIEM) // Столыпинский вестник. — 2022. — № 4. — С. 2121—2129.
7. A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN / N. Naik [et al.] // Contributions Presented at The International Conference on Computing, Communication, Cybersecurity and AI, July 3–4, 2024, London, UK. — Springer Nature Switzerland, 2024. — P. 271–280. — ISBN 9783031744433. — DOI: 10.1007/978-3-031-74443-3_16.
8. *Cecil R. R.*, *Soares J.* IBM Watson Studio: A Platform to Transform Data to Intelligence // Pharmaceutical Supply Chains — Medicines Shortages. — Springer International Publishing, 2019. — P. 183–192. — ISBN 9783030153984. — DOI: 10.1007/978-3-030-15398-4_13.
9. On metrics and prioritization of investments in hardware security. Systems Engineering / Z. A. Collier [et al.]. — 2023. — (Visited on 09/13/2025).
10. *Walha A.*, *Ghozzi F.*, *Gargouri F.* Data integration from traditional to big data: main features and comparisons of ETL approaches // The Journal of Supercomputing. — 2024. — Sept. — Vol. 80, no. 19. — P. 26687–26725. — ISSN 1573-0484. — DOI: 10.1007/s11227-024-06413-1.