БЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ ДОСТУПОМ В РАСПРЕДЕЛЁННЫХ БАЗАХ ДАННЫХ

Фёдоров Д.Д., Болтунов М.А.

Научный руководитель – Перова Марина Викторовна, Заведующая кафедрой информационных технологий ЮРИУ РАНХиГС

Южно-Российский институт управления – филиал РАНХиГС, г. Ростов-на-Дону

Аннотация: *В статье рассматриваются современные проблемы безопасности данных в распределённых базах данных, включая вызовы, вызванные географической распределённостью и репликацией данных. Основное внимание уделено актуальным угрозам, таким как кибератаки, утечки данных и нарушение консистентности. Обсуждаются современные методы защиты, включая шифрование, модели управления доступом, такие как Zero Trust, а также инструменты аналитики и обнаружения угроз. Статья также анализирует роль нормативно-правовых актов и государственных программ, таких как "Цифровая экономика", в обеспечении безопасности данных. Приводится оценка экономических аспектов защиты данных, подчеркивая важность инвестиций в безопасность для предотвращения финансовых потерь и репутационных рисков.*

Ключевые слова: *распределённые базы данных, безопасность данных, шифрование, управление доступом, Zero Trust, кибератаки, утечка данных, консистентность данных, блокчейн, искусственный интеллект, нормативно-правовые акты, цифровая экономика, SIEM-системы, аналитика угроз.*

В условиях стремительной цифровизации экономики и глобальной интеграции информационных технологий, распределённые базы данных становятся ключевыми компонентами инфраструктуры большинства современных организаций. Эти системы позволяют эффективно управлять большими объемами данных, обеспечивая их доступность и консистентность на географически удалённых узлах. Однако с ростом сложности и распространённости распределённых систем возрастает и количество угроз, связанных с безопасностью данных.

Актуальность темы безопасности и управления доступом в распределённых базах данных обусловлена несколькими факторами. Во-первых, с увеличением объёмов хранимых и передаваемых данных возрастает и риск их компрометации, что делает критически важным внедрение эффективных методов защиты. Во-вторых, с развитием технологий и методов обработки данных, таких как блокчейн и искусственный интеллект, встает задача обновления механизмов безопасности для обеспечения их соответствия новым вызовам.

Кроме того, важным аспектом является влияние нормативно-правовых актов (НПА) и государственных программ на обеспечение безопасности данных в распределённых системах. Программы, такие как "Цифровая экономика", а также федеральные законы № 152-ФЗ "О персональных данных" и № 149-ФЗ "Об информации, информационных технологиях и защите информации", задают основные направления и требования для защиты данных, что непосредственно влияет на безопасность распределённых баз данных.

Таким образом, управление безопасностью данных в распределённых системах требует комплексного подхода, включающего соблюдение законодательства, внедрение новых технологий защиты и постоянное обновление методов управления доступом.

Обеспечение безопасности данных в распределённых базах данных невозможно без учёта нормативно-правовой базы, регулирующей эту сферу. В России нормативно-правовые акты (НПА) и стандарты задают основы для защиты данных, устанавливают требования к организациям и определяют механизмы предотвращения и устранения угроз. Эти меры становятся особенно важными в контексте распределённых систем, где данные обрабатываются и хранятся на географически удалённых узлах, что повышает риски их утечки или повреждения.

Основные НПА, регулирующие информационную безопасность в России, включают следующие документы:

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ: Этот закон определяет требования к обработке персональных данных, включая необходимость их защиты от несанкционированного доступа и утечки. Закон предписывает операторам персональных данных внедрять организационные и технические меры защиты, что критически важно в распределённых системах, где персональные данные могут передаваться между узлами. [1]

2. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации": Закон охватывает широкий спектр вопросов, связанных с защитой информации, включая использование криптографических средств, установление правил доступа и предотвращение угроз для информационных систем. [2]

3. ГОСТы и рекомендации ФСТЭК России: ГОСТ Р 57580-2017: стандарт, регламентирующий защиту финансовых данных и определяющий базовые принципы обеспечения безопасности. Рекомендации ФСТЭК по защите распределённых систем: содержат методики оценки угроз и рекомендации по внедрению многоуровневой защиты.

Эти стандарты задают базу для построения системы управления безопасностью, включая использование средств шифрования, систем мониторинга и контроля доступа.

Экспертно-аналитический центр ГК InfoWatch (ЭАЦ) представил отраслевой отчет об утечках информации(Рис. 1). Отмечены тенденции по утечкам информации в мире и в России по следующим отраслям: Здравоохранение, ИТ и Телекоммуникации, Промышленность. Например, в Промышленности за 2023 год кратно выросло количество утечек информации в мире, а в России произошел сдержанный рост. Сфера Здравоохранения в мире демонстрирует рост количества утечек информации, при этом в России, после некоторого снижения в 2022 году, их стало больше в 2023 году. В то же время отрасль ИТ и Телекоммуникации показала устойчивый рост количества утечек данных в глобальном масштабе, но в России после существенного увеличения количества утечек в 2022 году последовал спад в 2023 году. [3]

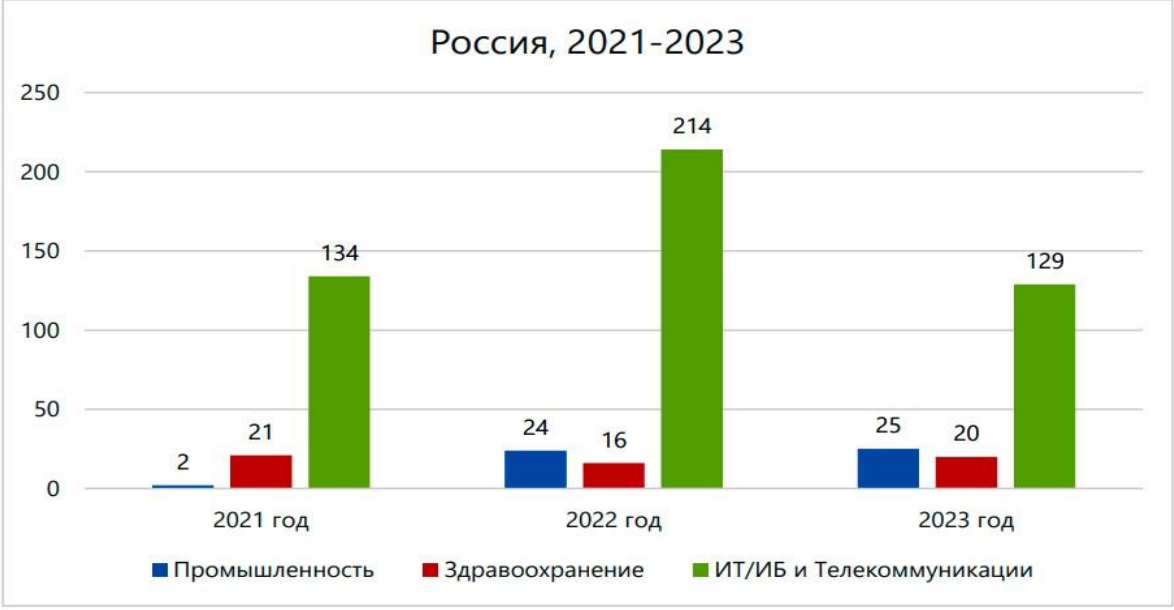

Рис. 1 – Россия, 2021-2023

Для стимулирования внедрения современных технологий защиты данных в распределённых системах реализуются программы и инициативы на государственном уровне. Наиболее значимыми из них являются:

1. Программа "Цифровая экономика": В рамках этой программы разработаны ключевые инициативы, направленные на защиту данных, в том числе в распределённых системах. В программе заложено финансирование исследований в области кибербезопасности, а также внедрение инструментов защиты информации в государственных и частных структурах.

2. Национальная стратегия по безопасности данных: Этот документ определяет приоритеты в области защиты данных, включая развитие технологий управления доступом и мониторинга угроз.

Кроме того, отдельное внимание уделяется импортозамещению в сфере программного обеспечения, включая решения для управления безопасностью баз данных. Российские разработчики активно работают над созданием платформ и инструментов, соответствующих национальным стандартам и требованиям.

Несмотря на наличие обширной нормативной базы, существуют определённые недостатки в регулировании безопасности распределённых баз данных:

1. Устаревание законодательных норм: Многие нормы НПА не успевают за развитием технологий. Например, они слабо учитывают особенности современных распределённых систем, таких как блокчейн или использование облачных технологий.

2. Недостаточная конкретизация требований: Некоторые законы дают лишь общие указания, оставляя организациям свободу в выборе методов защиты, что может приводить к неэффективной реализации мер безопасности.

3. Отсутствие стандартов для новых технологий: Технологии искусственного интеллекта и машинного обучения, которые активно используются для управления доступом и анализа угроз, пока недостаточно описаны в рамках существующих стандартов.

Для устранения этих недостатков необходимо разработать обновлённые НПА, адаптированные под современные вызовы, а также расширить использование международных стандартов, таких как ISO/IEC 27001, в российских организациях.

Таким образом, государственное регулирование играет ключевую роль в обеспечении безопасности распределённых баз данных. Комплексный подход, включающий совершенствование НПА, поддержку отечественных технологий и активное внедрение международных стандартов, создаёт основу для повышения уровня защиты данных в цифровой экономике.

Распределённые базы данных (РБД) являются основой для работы множества современных приложений и систем, от облачных сервисов до корпоративных информационных платформ. Их уникальные архитектурные особенности, такие как географическая распределённость и репликация данных, создают как новые возможности, так и специфические вызовы безопасности. Эти вызовы связаны с обеспечением конфиденциальности, целостности и доступности данных в условиях сложных угроз, включая кибератаки, утечки информации и внутренние ошибки.

Одной из ключевых характеристик распределённых баз данных является их способность хранить и обрабатывать данные на множестве узлов, расположенных в разных

географических зонах. Это повышает производительность и отказоустойчивость систем, но одновременно усложняет задачи защиты информации. [4]

1. Географическая распределенность: В распределённых системах данные передаются между узлами через публичные или частные сети, что делает их уязвимыми для перехвата или модификации. Защита таких передач требует использования методов шифрования и протоколов безопасной связи, таких как TLS. Однако недостаточная настройка или использование устаревших алгоритмов шифрования может привести к утечкам.

2. Репликация данных: Для обеспечения высокой доступности распределённые базы данных копируют данные между узлами. Это уменьшает риск потери информации при сбоях, но создает вызовы, связанные с консистентностью данных. Конфликтующие изменения, сделанные на разных узлах, могут нарушить целостность данных. Кроме того, каждый экземпляр реплики данных увеличивает поверхность атаки, увеличивая риск утечек или компрометации.

Основные угрозы:

1. Кибератаки: Распределённые базы данных часто становятся мишенью кибератак, нацеленных на нарушение их работы или доступ к данным. Среди них распространены DDoS-атаки, перегружающие узлы и делая систему недоступной, что особенно опасно для распределённых систем. SQL-инъекции позволяют злоумышленникам внедрять вредоносный код через уязвимые интерфейсы API или веб-приложения, получая доступ к данным или изменяя их. Атаки, использующие уязвимости ПО, эксплуатируют ошибки в коде, устаревшие библиотеки или неподдерживаемые системы, что открывает доступ для взлома. Для защиты необходимы регулярные обновления, валидация запросов и современные механизмы обнаружения угроз.

2. Утечки данных: В распределённых системах утечки данных могут происходить на любом этапе их обработки или передачи. Одной из основных причин является компрометация узла системы, которая может произойти как через физический доступ к оборудованию, так и через удалённое проникновение, например, с использованием уязвимостей в программном обеспечении. Ещё одной частой причиной утечек является неправильная настройка доступа, когда чувствительная информация становится доступной для широкого круга пользователей или даже через интернет. Внутренние угрозы также играют значительную роль, когда сотрудники злоупотребляют своими полномочиями или случайно передают данные третьим лицам. Такие утечки могут быть особенно опасными, так как часто они происходят без ведома организации, что делает их трудными для обнаружения и предотвращения.

3. Нарушение консистентности: может возникать, например, при одновременном доступе нескольких пользователей к одной и той же информации и её корректировке. В таком случае есть опасность искажения данных. [5]

Анализ реальных инцидентов показывает, что большинство угроз безопасности в распределённых системах связаны с человеческими ошибками, недостаточным уровнем защиты и сложностью архитектуры. Например:

1. В 2020 году один из крупнейших инцидентов с утечкой данных произошёл из-за неправильно настроенной распределённой базы данных Elasticsearch, что позволило злоумышленникам получить доступ к миллионам записей.

2. В 2021 году уязвимость в Apache Cassandra, популярной распределённой СУБД, позволила злоумышленникам удалённо выполнять команды на серверах, получая полный контроль над узлами.

3. В банковской сфере были зафиксированы случаи, когда DDoS-атаки на распределённые базы данных привели к отказу в обслуживании клиентов и многомиллионным убыткам.

Безопасность распределённых баз данных требует комплексного подхода, учитывающего их уникальные особенности. Географическая распределённость и репликация данных создают дополнительные риски, связанные с защитой каналов связи и поддержанием консистентности. Основные угрозы, такие как кибератаки и утечки, остаются актуальными и требуют внедрения передовых технологий защиты, постоянного мониторинга и своевременного обновления программного обеспечения. Анализ инцидентов показывает важность обучения персонала и использования автоматизированных инструментов для обнаружения и предотвращения угроз.

Методы шифрования и управления ключами:

Шифрование — это сокрытие или видоизменение данных таким образом, чтобы другие люди не могли их прочитать или понять. Даже если злоумышленникам удастся украсть зашифрованную информацию, они не смогут её использовать, не разгадав код. На практике для защиты данных в РБД используются следующие методы шифрования:

1. Шифрование данных в покое (at-rest encryption): Этот метод применяется для защиты данных, когда они находятся на дисках или в хранилищах. Наиболее распространёнными алгоритмами для шифрования в покое являются AES (Advanced Encryption Standard) и RSA. Важно, чтобы ключи шифрования хранились отдельно от самих данных, что повышает уровень безопасности.

2. Шифрование данных в передаче (in-transit encryption): Для защиты данных, передаваемых между узлами распределённой базы данных, используется шифрование на

уровне транспортных протоколов. Одним из самых распространённых решений является использование TLS (Transport Layer Security), который гарантирует защиту данных от перехвата или модификации во время их передачи по открытым сетям.

3. Шифрование на уровне полей (field-level encryption): В некоторых случаях может потребоваться шифрование отдельных полей данных (например, персональных данных) для обеспечения дополнительной защиты. Этот метод позволяет ограничить доступ к чувствительной информации даже при наличии доступа к базе данных.

Кроме того, важно правильно управлять ключами шифрования, используя специальные системы управления ключами (KMS, Key Management Systems). Эти системы обеспечивают безопасное хранение и использование ключей, предотвращая их утечку или несанкционированное использование.

В последние годы активно развиваются новые подходы к обеспечению безопасности данных в распределённых системах. Одним из таких решений является блокчейн, который предоставляет механизм защиты данных с помощью технологии распределённого реестра. Блокчейн позволяет обеспечить неизменность и прослеживаемость данных, делая их невосприимчивыми к изменениям и манипуляциям.[6]

Защита данных в распределённых системах и базах данных продолжает развиваться, и современные решения становятся всё более сложными и многогранными. В условиях цифровизации, когда данные становятся одним из самых ценных ресурсов, обеспечение их безопасности выходит на первый план. Важной составляющей такого процесса является не только использование эффективных технологий защиты, но и аналитика, направленная на прогнозирование будущих угроз и улучшение существующих решений. В этом разделе рассматриваются основные направления, в которых развивается безопасность в распределённых базах данных, а также экономические аспекты, связанные с затратами на защиту данных и их последствиями для бизнеса.

Современные технологии защиты данных в распределённых системах продолжают развиваться. Рассмотрим несколько ключевых направлений:

1. Шифрование. Остаётся основным способом защиты данных, и его развитие направлено на улучшение производительности и снижение затрат на управление ключами. В будущем ожидается рост использования гомоморфного шифрования, которое позволяет выполнять вычисления на зашифрованных данных, что важно для безопасных облачных вычислений. Однако эта технология требует значительных вычислительных ресурсов, и её использование станет более доступным с развитием аппаратных ускорителей, таких как FPGA и ASIC.

2. Модели управления доступом (RBAC, ABAC, Zero Trust). Модель Zero Trust набирает популярность благодаря своей эффективности в децентрализованных системах. В отличие от традиционного подхода, Zero Trust требует постоянной аутентификации и авторизации для каждого запроса. Ожидается, что в будущем эта модель будет интегрирована с искусственным интеллектом, что повысит адаптивность и автоматизацию контроля доступа.

3. Инструменты аналитики и обнаружения угроз. Использование SIEM-систем для мониторинга безопасности продолжает расти. В будущем аналитические инструменты будут интегрированы с машинным обучением и искусственным интеллектом для более точного и своевременного обнаружения угроз. Прогнозируется, что такие системы будут использовать предсказательную аналитику для предотвращения атак до их возникновения.

С каждым годом затраты на безопасность данных становятся всё более значительными для организаций. Включение новых технологий в защиту данных требует не только значительных инвестиций в программное обеспечение и оборудование, но и в обучении сотрудников, а также в обновлении инфраструктуры.

Внедрение современных технологий безопасности, таких как гомоморфное шифрование или интеграция AI в системы мониторинга, требует больших капиталовложений. Компании должны балансировать между безопасностью и затратами, при этом понимая, что отсутствие должной защиты может привести к значительным убыткам в случае утечки данных или кибератаки. Важно, что инвестиции в безопасность данных могут стать оправданными с точки зрения долгосрочной выгоды, если они предотвращают финансовые потери, штрафы и утрату репутации.

В распределённых системах безопасность данных может потребовать больших усилий для мониторинга и защиты множества узлов. Однако с ростом масштабируемости и автоматизацией процессов защиты данных организации могут снизить затраты. Например, интеграция SIEM-систем и использование облачных решений для защиты данных позволяют значительно снизить расходы на локальную инфраструктуру и повысить гибкость систем безопасности. В будущем такие решения могут стать ещё более доступными и эффективными благодаря улучшению алгоритмов, искусственного интеллекта и облачных технологий.

Важной частью экономического анализа является оценка рисков. Несоответствие требованиям безопасности или утечка данных может привести к штрафам, судебным разбирательствам и утрате доверия со стороны клиентов. Статистика показывает, что финансовые потери от утечек данных могут составлять миллиарды долларов, что подчеркивает необходимость инвестировать в надёжную защиту. Более того, компании,

которые эффективно обеспечивают безопасность данных, могут использовать это как конкурентное преимущество, продвигая свою репутацию как надёжного партнёра.

Таким образом, обеспечение безопасности данных в распределённых системах является важнейшей задачей в условиях цифровизации экономики. Географическая распределённость и репликация данных создают как возможности для повышения отказоустойчивости, так и дополнительные риски, связанные с утечками, кибератаками и нарушением консистентности. Актуальность защиты данных усиливается в свете развития новых технологий, таких как блокчейн и искусственный интеллект, что требует обновления нормативно-правовых актов и внедрения современных методов шифрования, управления доступом и аналитики угроз. Внедрение таких решений требует значительных затрат, но в долгосрочной перспективе инвестиции в безопасность данных становятся оправданными, предотвращая финансовые потери и укрепляя репутацию организаций.

Список литературы

1. Федеральный закон Российской Федерации "О персональных данных" от 27.07.2006 N 152-ФЗ. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 27 ноября 2024).

2. Федеральный закон Российской Федерации № 149-ФЗ "Об информации, информационных технологиях и о защите информации". — URL: https://www.consultant.ru/document/cons_doc_LAW_61712/ (дата обращения: 27 ноября 2024).

3. Исследование утечек информации в отраслях за три года. — URL: https://www.infow.ru/analytics/analitika/issledovaniye-uteche-informatsii-v-otraslyakh-za-tri-goda (дата обращения: 13.12.2024).

4. Лемехов, А. В. Информационная безопасность распределённых систем: теория и практика. — М.: ЭКМО, 2020.

5. Борисов, В. И., Козлов, А. В. "Безопасность распределённых систем: угрозы и методы защиты." // Журнал "Информационная безопасность", 2021. № 4. С. 23-35.

6. Шевченко, С. П. Архитектура распределённых баз данных и проблемы безопасности. — М.: РГТУ, 2019.