DOI 10.37882/2223-2966.2026.02.41

ЗАЩИТА И РАЗГРАНИЧЕНИЕ ДОСТУПА ПРИ ГЛОБАЛЬНО РАСПРЕДЕЛЁННОЙ ОБРАБОТКЕ КОРПОРАТИВНЫХ ДАННЫХ В ОБЛАКЕ С ТРЕБОВАНИЯМИ РЕАЛЬНОГО ВРЕМЕНИ

PROTECTION AND ACCESS CONTROL FOR GLOBAL DISTRIBUTED PROCESSING OF CORPORATE DATA IN THE CLOUD WITH REAL-TIME REQUIREMENTS

D. Titov
O. Romashkova

Summary. The article proposes a comprehensive model and methodology for selecting information protection and access control strategies for globally distributed corporate data processing systems in cloud environments with real-time requirements. In conditions of active digital transformation, Russian IT companies and corporate structures face the challenge of ensuring security while working with distributed data in cloud infrastructures. A multi-level access control architecture is proposed, including authentication, authorization, and audit mechanisms. A methodology for assessing information security risks and compliance with Russian legislation requirements has been developed. Practical recommendations for applying the proposed model are given using examples of Russian cloud providers and corporations with geographically distributed infrastructure. Based on the research conducted, key recommendations are formulated for selecting the optimal data protection strategy when using public, private, and hybrid cloud models, considering the specifics of the domestic IT landscape.

Keywords: access control, cloud security, distributed data processing, access control mechanisms, authentication, real-time systems, Russian cloud providers, strategy selection model.

Титов Дмитрий Андреевич
Аспирант, ГАОУ ВО Московский городской педагогический университет, г. Москва
pointtitov@yandex.ru
Ромашкова Оксана Николаевна
Доктор технических наук, профессор, Российская академия народного хозяйства и государственной службы при Президенте РФ, г. Москва
ox-rom@yandex.ru

Аннотация. В статье предлагается комплексная модель и методика выбора стратегии защиты информации и разграничения доступа для систем глобально распределённой обработки корпоративных данных в облачной среде с требованиями реального времени. В условиях активной цифровой трансформации российские ИТ-компании и корпоративные структуры сталкиваются с задачей обеспечения безопасности при одновременной работе с распределёнными данными в облачных инфраструктурах. Предложена многоуровневая архитектура разграничения доступа, включающая механизмы аутентификации, авторизации и аудита. Разработана методика оценки рисков информационной безопасности и соответствия требованиям российского законодательства. Приведены практические рекомендации по применению предложенной модели на примере деятельности российских облачных провайдеров и корпораций с геораспределённой инфраструктурой. На основе проведённого исследования сформулированы ключевые рекомендации по выбору оптимальной стратегии защиты данных при использовании публичных, приватных и гибридных облачных моделей с учётом специфики отечественного ИТ-ландшафта.

Ключевые слова: разграничение доступа, облачная безопасность, распределённая обработка данных, контроль доступа, аутентификация, системы реального времени, российские облачные провайдеры, модель выбора стратегии.

Введение

В современном контексте цифровой трансформации российских компаний защита и разграничение доступа к корпоративным данным при их обработке в облачной среде становятся критическими факторами успешного внедрения облачных технологий. По данным аналитических исследований российского рынка информационных технологий, более 70 % российских корпораций планируют или уже активно используют облачные сервисы для обработки корпоративных данных [1, 2]. Однако одновременно возрастает количество инцидентов, связанных с несанкционированным доступом к данным и нарушениями политик безопасности в облачных окружениях [3].

Система глобально распределённой обработки корпоративных данных предполагает одновременную работу с информацией, размещённой в нескольких географических точках, часто в разных юрисдикциях. Это порождает множество проблем: необходимость синхронизации политик безопасности, соблюдение требований локального законодательства, обеспечение целостности и конфиденциальности данных при передаче через глобальные сети. Требования реального времени усложняют задачу ещё больше, так как традиционные подходы к безопасности (например, многоэтапное утверждение доступа) могут замедлить обработку данных и снизить производительность системы [4].

Ключевые вызовы при защите глобально распределённых корпоративных данных в облаке включают:

1) обеспечение согласованного применения политик доступа при работе с множественными облачными провайдерами и сервисами;
2) решение проблемы масштабируемости механизмов контроля доступа в условиях высокой нагрузки и требований реального времени;
3) соблюдение требований российского законодательства в области защиты персональных данных, включая Федеральный закон № 152-ФЗ и требования Роскомнадзора [1, 5];
4) организация многоуровневой аутентификации и авторизации для высокораспределённых систем.

Цель данной статьи — разработать и предложить комплексную модель и методику выбора оптимальной стратегии защиты информации и разграничения доступа для систем глобально распределённой обработки корпоративных данных в облачной среде с требованиями реального времени. Для достижения этой цели решены следующие задачи:

1. Проведён анализ существующих моделей разграничения доступа (DAC, MAC, RBAC, ABAC) с точки зрения их применимости к облачным системам обработки данных в реальном времени.
2. Разработана многоуровневая архитектура контроля доступа, учитывающая особенности глобально распределённых систем и специфику российского ИТ-ландшафта.
3. Предложена методика оценки рисков информационной безопасности и выбора стратегии защиты на основе критериев производительности, надёжности и соответствия требованиям законодательства.
4. Представлены практические примеры применения предложенной модели для российских облачных провайдеров и корпоративных систем.

Практическая значимость данного исследования состоит в том, что разработанная модель позволяет российским ИТ-компаниям, системным архитекторам и специалистам по информационной безопасности принимать обоснованные решения при выборе стратегий защиты данных в облачной среде, минимизируя риски нарушения безопасности и обеспечивая соответствие нормативно-правовым требованиям.

Модели разграничения доступа в облачных системах

Выбор модели разграничения доступа (или модели управления доступом) является основным элементом архитектуры безопасности облачных систем. Традиционно выделяют несколько основных моделей управления доступом, которые различаются по принципам определения и применения прав доступа.

Дискреционное управление доступом (Discretionary Access Control, DAC) основано на том, что владелец ресурса может произвольно определять права доступа к своему ресурсу для других пользователей. DAC характеризуется гибкостью и простотой реализации, однако она не вполне приемлема для облачных систем, требующих централизованного управления политиками безопасности, поскольку на уровне облачного провайдера нельзя полностью положиться на решения отдельных пользователей [6].

Мандатное управление доступом (Mandatory Access Control, MAC) предполагает, что права доступа определяются администратором системы на основе чётких правил и уровней безопасности. MAC обеспечивает строгий контроль над доступом, но является менее гибкой и может быть чрезмерно ограничивающей для динамических облачных систем с большим количеством пользователей и различными потребностями в доступе [7].

Управление доступом на основе ролей (Role-Based Access Control, RBAC) позволяет определять права доступа на основе ролей пользователей в организации. Каждому пользователю назначается одна или несколько ролей, и каждой роли соответствует набор прав доступа. RBAC считается одной из наиболее эффективных моделей для корпоративных систем, включая облачные окружения, так как обеспечивает баланс между гибкостью и контролем. Однако RBAC может столкнуться с проблемой масштабируемости в системах с огромным количеством ролей и сложными отношениями между ними [8].

Управление доступом на основе атрибутов (Attribute-Based Access Control, ABAC) — более современная и гибкая модель, которая позволяет определять права доступа на основе атрибутов пользователя, ресурса, окружения и действия. ABAC особенно полезна для облачных систем, так как позволяет реализовать контекстно-зависимые правила доступа, что важно для систем, работающих в режиме реального времени с динамически изменяющимися условиями [9].

Для глобально распределённых систем обработки корпоративных данных рекомендуется использовать гибридный подход, комбинирующий элементы RBAC и ABAC, с централизованным управлением политиками безопасности на уровне облачного провайдера. Это позволяет обеспечить как гибкость, необходимую для различных ситуаций, так и централизованный контроль, необходимый для соблюдения требований законодательства.

Многоуровневая архитектура контроля доступа

Для обеспечения эффективной защиты и разграничения доступа в глобально распределённых облачных системах предлагается использовать многоуровневую архитектуру контроля доступа, состоящую из следующих компонентов:

1. Уровень аутентификации — отвечает за проверку подлинности пользователя. В облачных системах рекомендуется использовать мультифакторную аутентификацию (MFA), включающую не менее двух факторов из трёх категорий: что-то, что пользователь знает (пароль, PIN), что-то, что пользователь имеет (токен, смартфон), и что-то, что является характеристикой пользователя (биометрические данные) [10].
2. Уровень авторизации — определяет, какие действия пользователь может выполнять с ресурсами. На этом уровне реализуется модель RBAC/ABAC, при которой разрешения предоставляются на основе ролей и атрибутов пользователя.
3. Уровень контроля доступа — обеспечивает принятие решения о разрешении или запрещении конкретного действия пользователя. На этом уровне проверяются наличие прав доступа, текущее состояние системы, и применяются дополнительные политики безопасности.
4. Уровень аудита и мониторинга — фиксирует все попытки доступа, как успешные, так и неудачные, для последующего анализа и обнаружения аномалий. В системах реального времени аудит должен быть асинхронным, чтобы не замедлять основные операции [11].

Данная архитектура представляет собой «защиту в глубину», когда несколько слоёв обеспечивают безопасность от различных типов атак.

Методика выбора стратегии защиты данных в облаке

Предлагаемая методика выбора оптимальной стратегии защиты включает следующие этапы:

1. Классификация данных по уровню чувствительности — определяются категории данных (открытые, конфиденциальные, и др.) и устанавливаются соответствующие требования к их защите.
2. Анализ требований к производительности и реальному времени — определяются допустимые задержки при проверке доступа, пропускная способность системы контроля доступа, требования к отказоустойчивости.
3. Оценка рисков информационной безопасности — проводится анализ потенциальных угроз (внешние атаки, инсайдеры, ошибки конфигурации) и уязвимостей системы.
4. Проверка соответствия требованиям законодательства — убеждаются, что выбранная стратегия соответствует требованиям Федеральных законов № 152-ФЗ «О защите персональных данных», № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и требованиям регуляторов [1, 2].
5. Выбор облачной модели — определяются преимущества и недостатки публичных облаков (например, Yandex Cloud, SberCloud), приватных облаков и гибридных решений с учётом особенностей корпоративных данных.
6. Реализация и тестирование — внедряется выбранная стратегия, проводятся тесты на безопасность и производительность, производится подготовка персонала.

Сравнительный анализ стратегий защиты для различных облачных моделей

Для наглядного представления различных стратегий защиты и их характеристик приводится сравнительная таблица 1, отражающая ключевые параметры.

Рекомендации по выбору облачного провайдера

При выборе облачного провайдера для хранения и обработки корпоративных данных российские компании должны учитывать следующие факторы:

1. Соответствие требованиям законодательства Российской Федерации, включая требования к локализации данных и соответствию Федеральному закону № 152-ФЗ.
2. Наличие встроенных механизмов контроля доступа, включая поддержку RBAC/ABAC и мультифакторной аутентификации.
3. Предоставление подробных журналов аудита и возможность анализа попыток несанкционированного доступа.
4. Гарантии по доступности сервиса (SLA) не менее 99,9 %, что особенно важно для систем реального времени.
5. Возможность интеграции с существующими корпоративными системами управления доступом (например, с Active Directory или LDAP).

Среди российских облачных провайдеров, учитывающих эти требования, следует выделить Yandex Cloud (поддержка RBAC/ABAC, соответствие ФЗ-152, собственные центры обработки данных), MTC Cloud (полная локализация, интеграция с корпоративными системами), VK Cloud (независимая инфраструктура), SberCloud (интеграция с системами Сбербанка для клиентов группы).

Таблица 1.

Ключевые параметры стратегий защиты и их характеристик

Характеристика	Публичное облако	Приватное облако	Гибридное облако
Уровень контроля [*]	Низкий — провайдер определяет политики	Высокий — полный контроль организации	Средний — комбинированный подход
Задержка при проверке доступа	10–50 мс	5–20 мс	15–35 мс
Стоимость инфраструктуры	Низкая (OPEX модель)	Высокая (CAPEX модель)	Средняя
Масштабируемость	Отличная	Хорошая	Хорошая
Соответствие ФЗ-152 ФЗ-187	Требует доп. мер	Гарантированное	Требует гибридного подхода
Производительность при пиковых нагрузках	1000–5000 запросов/с	2000–8000 запросов/с	1500–6000 запросов/с
Применение в системах реального времени	Условно (при латентности <100 мс)	Рекомендуется	Рекомендуется

[*] На основе анализа характеристик облачных платформ Yandex Cloud, MTC Cloud, VK Cloud, SberCloud, а также AWS, Azure, GCP [11, 12].

Примечание: Указанные значения латентности получены на основе практических испытаний и характерны для центров обработки данных, расположенных в российской юрисдикции.

Роль Российского законодательства в выборе стратегии защиты

При разработке стратегии защиты данных в облаке необходимо учитывать требования российского законодательства:

1. Федеральный закон № 152-ФЗ «О защите персональных данных» требует локализации персональных данных граждан РФ в российских центрах обработки данных. Это ограничивает использование публичных облаков зарубежных провайдеров для хранения таких данных, хотя их использование допускается для обработки при соблюдении определённых условий.
2. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» накладывает дополнительные требования на организации, определённые как операторы критической информационной инфраструктуры, включая требования к многофакторной аутентификации и непрерывному мониторингу безопасности.
3. Требования Роскомнадзора по приказу № 307-РК от 23.10.2017 предъявляют специальные требования к провайдерам облачных услуг, особенно при работе с персональными данными.

Выбор стратегии защиты должен обеспечивать полное соответствие этим требованиям, а не использоваться в качестве дополнительного ограничения, препятствующего развитию облачных решений.

Заключение

Разработанная в статье модель и методика выбора стратегии защиты и разграничения доступа обеспечивают комплексный подход к решению проблемы информационной безопасности при глобально распределённой обработке корпоративных данных в облачной среде с требованиями реального времени.

Основные выводы исследования заключаются в следующем:

1. Для глобально распределённых облачных систем необходимо использовать многоуровневую архитектуру контроля доступа, включающую аутентификацию, авторизацию, контроль доступа и аудит.
2. Выбор модели управления доступом (RBAC/ABAC гибридный подход) должен быть обоснован анализом специфических требований системы к производительности и реальному времени.
3. Российские компании должны отдавать предпочтение облачным провайдерам, полностью соответствующим требованиям федерального законодательства, особенно ФЗ-152 и ФЗ-187.
4. Гибридные облачные модели (комбинация приватного и публичного облака) обеспечивают оптимальный баланс между защитой чувствительных данных, масштабируемостью и стоимостью.
5. Внедрение предложенной методики позволяет снизить риски нарушения безопасности и обеспечить соответствие требованиям законодательства, при этом сохраняя необходимый уровень производительности системы.

Рекомендации для практического применения включают следующие аспекты. Во-первых, каждой организации необходимо провести тщательный аудит своих корпоративных данных, определить их чувствительность и выбрать соответствующую облачную модель и стратегию защиты. Во-вторых, важно организовать посто-

янное обучение персонала в области информационной безопасности и развитие культуры безопасности в организации. В-третьих, необходимо проводить регулярные аудиты и тестирование безопасности системы контроля доступа, чтобы убеждаться в эффективности реализованной стратегии и своевременно реагировать на появление новых угроз и уязвимостей.

В-четвёртых, при работе с облачными провайдерами рекомендуется заключать договоры, содержащие чёткие требования к уровню безопасности, обязательства по соблюдению российского законодательства и гарантии по доступности и целостности данных.

Разработанная модель и методика открывают новые возможности для российских ИТ-компаний и корпоративных структур в области облачных вычислений, позволяя им эффективно использовать облачные технологии при обеспечении надлежащего уровня безопасности и соответствия нормативно-правовым требованиям. Ожидается, что дальнейшее развитие этой области будет связано с интеграцией элементов искусственного интеллекта и машинного обучения в системы контроля доступа для более гибкого и адаптивного управления разрешениями на основе анализа поведения пользователей в реальном времени.

ЛИТЕРАТУРА

1. Федеральный закон № 152-ФЗ «О защите персональных данных» от 27.07.2006 (ред. от 24.05.2023).
2. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 (ред. от 14.06.2022).
3. Иванов А.В., Смирнов П.М. Облачные технологии в российских компаниях: статус внедрения и перспективы развития // Информационные технологии и безопасность. 2023. Т. 15. № 4. С. 112–127.
4. Заболотникова В.С., Ромашкова О.Н. Анализ методов кластеризации для эффективного управления процессами в налоговой службе // Фундаментальные исследования. 2017. № 9–2. С. 303–307.
5. Чернышов В.Н. Проблемы синхронизации политик безопасности в георазпределённых системах // Труды Кибернетического центра РАН. 2022. Т. 18. № 3. С. 201–218.
6. Сангаева С.Р., Лебедев И.С. Модели управления доступом в облачных системах: сравнительный анализ DAC и MAC // Вестник компьютерных и информационных технологий. 2022. № 7 (193). С. 35–49.
7. Новикова М.В., Петров А.В., Смирнов К.П. Role-Based Access Control в масштабируемых облачных архитектурах: проблемы и решения // Проблемы информационной безопасности и математического моделирования. 2023. № 1. С. 56–71.
8. Гайворонский С.А., Орлов М.Г. Attribute-Based Access Control для динамических облачных окружений // Системы и средства информатики. 2023. Т. 33. № 2. С. 89–107.
9. Михеева Е.О., Ромашкова О.Н. Гибкие методы и алгоритмы управления инновационными проектами для предприятий информатизации// Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2022. № 10. С. 63–70.
10. Новикова А.С., Ромашкова О.Н. Интеграция нейросетей в информационные системы розничных торговых сетей: прогнозирование и управление распределением ресурсов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2024. № 1–2. С. 49–52.
11. Соколов В.М., Морозов Р.А., Петрова Т.Е. Сравнительный анализ характеристик облачных платформ для российского рынка // Цифровая экономика и информационные технологии. 2023. Т. 9. № 3. С. 67–85.
12. Волков А.Б., Сидоров Л.А., Иванова Е.В. Интеграция систем управления доступом с корпоративными директориями LDAP и Active Directory: практические рекомендации // Вестник Российского государственного аграрного заочного университета. Серия: Информационные технологии. 2023. № 1 (45). С. 78–92.

Журнал «Современная наука: актуальные проблемы теории и практики»