Открытый журнал евразийских исследований, 2026, №3, сс. 110-128
doi: 10.65469/eijournal.2026.3.12
eijournal.ilimbilim.kg

ИНФОРМАТИКА / COMPUTER SCIENCE
УДК 004.056

Защита данных в распределённых и облачных серверных системах (на примере финансового сектора)

Омаралиева Гулбайра Абдималиковна
Ошский государственный университет, Кыргызстан, gulya@oshsu.kg, ORCID: 0000-0003-1862-2142

Мамасалиев Ажибек Арзиматович
Ошский государственный университет, Кыргызстан, azhibekmamasaliev@gmail.com, ORCID: 0009-0004-9159-4357

Абдыкадыров Султанбек Каныбекович
Ошский государственный университет, Кыргызстан, sultanbekabdykadyrov69@gmail.com, ORCID: 0009-0001-7078-4686

Аннотация
Организации финансового сектора всё чаще переносят серверные системы в распределённую и облачную среду, что обусловлено требованиями к масштабируемости, отказоустойчивости и скорости вывода продуктов на рынок. Обработка данных за пределами собственного периметра создаёт риски для конфиденциальности и целостности, усиливает зависимость от провайдера и требует явного учёта границ доверия и управления ключами шифрования. Недостаточная проработка этих аспектов ведёт к инцидентам, нарушению тайны банковских операций и несоответствию отраслевым стандартам.

Ключевые слова: защита данных, распределённые системы, облачные вычисления, границы доверия, KMS, HSM, BYOK, модель разделённой ответственности, информационная безопасность

Для цитирования: Омаралиева Г.А., Мамасалиев А.А., Абдыкадыров С.К. (2026). Защита данных в распределённых и облачных серверных системах (на примере финансового сектора). *Открытый журнал евразийских исследований*, №3, сс. 110-128. doi: 10.65469/eijournal.2026.3.12

Введение

Распределённые и облачные серверные системы широко применяются в финансовом секторе для размещения приложений, баз данных и платёжной инфраструктуры [1; 2]. Переход от монолитных локальных развёртываний к сервисно-ориентированным архитектурам в распределённых средах стал устойчивой тенденцией последнего десятилетия: банки, процессинговые центры, платёжные агрегаторы и микрофинансовые организации размещают ядро автоматизированной банковской системы, фронтальные каналы и аналитические

контуры в виртуализированных средах, а часть нагрузок передают внешним провайдерам облачных сервисов. Преимущества такого подхода — эластичность вычислительных ресурсов, сокращение капитальных затрат, ускоренный выпуск продуктов и возможность резервирования по нескольким географическим зонам — сопровождаются совокупностью рисков, отсутствующих в классическом on-premise периметре.

Ключевое изменение при переходе в облако состоит в смещении границ доверия (trust boundaries): данные обрабатываются на вычислительных ресурсах провайдера, ключи шифрования могут находиться под контролем третьей стороны, а мультитенантная архитектура создаёт дополнительные угрозы изоляции и утечки между заказчиками. Провайдер получает часть функций, традиционно закреплённых за собственной службой информационной безопасности организации: физическую защиту, управление гипервизором, обновление операционных систем в управляемых сервисах, а в случае SaaS — ещё и управление прикладным кодом [3; 8]. Это требует переосмысления модели ответственности: в распределённой среде безопасность становится совместной функцией заказчика и провайдера, а её распределение должно быть явно зафиксировано в договоре, технических регламентах и архитектурных решениях.

Международные стандарты и отраслевые руководства формулируют требования к защите информации в облаке, но оставляют значительную свободу в выборе конкретных мер. ISO/IEC 27001:2022 требует наличия системы менеджмента информационной безопасности и периодической оценки рисков; NIST SP 800-53 Rev. 5 задаёт каталог из более чем тысячи контролей, охватывающих все функциональные области защиты; NIST SP 800-144 содержит отдельные рекомендации по безопасности публичных облаков; PCI DSS v4.0 регулирует обработку данных платёжных карт и явно предъявляет требования к шифрованию, разграничению доступа и логированию [3; 4; 11; 12]. В Кыргызской Республике финансовые организации дополнительно руководствуются требованиями Национального банка к обеспечению информационной безопасности и тайны банковских операций, что повышает значимость методологических подходов, позволяющих соотносить архитектурные решения с конкретными контролями.

Отдельное внимание специалисты уделяют угрозам, специфичным именно для распределённых и облачных сред. Отчёт Cloud Security Alliance «Top Threats to Cloud Computing — Pandemic Eleven» выделяет, в частности, недостаточное управление идентификацией и правами доступа, небезопасные интерфейсы и API, конфигурационные ошибки, слабый контроль за плоскостью управления, инсайдерские угрозы со стороны сотрудников провайдера и ограниченную видимость облачных нагрузок [13]. Работы [9; 10; 14] фиксируют, что именно компрометация учётных записей администраторов и ошибки конфигурации хранилищ становятся наиболее частыми причинами инцидентов в облачных развёртываниях банков и финтех-компаний. В этих условиях классические меры защиты периметра оказываются недостаточными, а центральное место занимают криптографическая защита данных, управление ключами и строгий контроль плоскости управления.

Для финансовых организаций Кыргызской Республики и сопредельных стран вопрос о переносе систем в облако приобретает дополнительные измерения. С одной стороны, ограниченный объём собственного рынка и высокая стоимость владения собственным центром обработки данных создают экономическое давление в пользу использования услуг

внешних провайдеров; с другой — требования к тайне банковских операций, к хранению данных клиентов внутри страны и к независимому аудиту существенно сужают множество допустимых моделей развёртывания. Сопоставление экономических и регуляторных факторов на этапе проектирования требует формализованной методики, которая позволила бы соотнести архитектурные решения с конкретными контролями стандартов и получить количественные оценки остаточного риска, сопоставимые между различными сценариями. Разработке такой методики и посвящена настоящая работа.

Научная новизна состоит в сочетании четырёхзонной модели защиты с реестром рисков, построенным по шкалам P и I, и с прямым отображением мер защиты на контроли ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5 и PCI DSS v4.0. В отличие от работ, посвящённых отдельным аспектам облачной безопасности [3; 9; 14], предлагаемый подход даёт сквозное представление от архитектурных решений до критериев соответствия и сопровождается количественным сравнением моделей развёртывания, что делает его пригодным для использования в проектировании и при подготовке к аудитам.

Целью работы является систематизация подходов к защите данных в распределённых и облачных серверных системах применительно к финансовому сектору и сравнительная оценка моделей развёртывания по критериям контроля над данными и ключами. Для достижения цели решаются задачи: описать типовую архитектуру с выделением границ доверия и зон защиты; классифицировать угрозы и сопоставить их с рекомендуемыми мерами; рассмотреть подходы к шифрованию и управлению ключами в облаке (in-transit, at-rest, BYOK, HYOK, envelope encryption); сопоставить меры защиты с контролями ISO/IEC 27001:2022 и NIST SP 800-53 Rev. 5; выполнить количественное сравнение on-premise, гибридной и публичной моделей развёртывания; сформулировать практические рекомендации. В статье последовательно излагаются материалы и методы, архитектура и границы доверия, угрозы и меры защиты, шифрование и управление ключами, сравнение моделей, обсуждение результатов, заключение и список литературы.

Материалы и методы исследования

Теоретической основой послужили работы исследователей ОшГУ по информационной безопасности, облачным технологиям и разработке веб-приложений [1; 2; 5; 6], публикации российских авторов по защите данных в распределённых системах [7; 9; 10], зарубежные стандарты и руководства (NIST SP 800-53 Rev. 5, NIST SP 800-144, NIST SP 800-57 Part 1 Rev. 5, ISO/IEC 27001:2022, ISO/IEC 27017:2015, PCI DSS v4.0) и научные статьи по облачной безопасности [3; 4; 8; 11–14]. Законы и подзаконные акты в список литературы не включались; соответствие регуляторным требованиям достигается выполнением стандартов и договорных обязательств с провайдером.

Модель исследования основана на типовой архитектуре распределённой и облачной системы с четырьмя логическими зонами: клиент, периметр, облачный провайдер, зона данных. Границы доверия проводятся между зонами и определяют момент передачи контроля над данными и ключами шифрования. Для сравнения рассмотрены три модели развёртывания: on-premise (все компоненты в периметре организации, собственный ЦОД и собственные HSM-модули), гибридное облако, публичное облако.

Критерии сравнения моделей: уровень контроля над ключами шифрования, наличие и модель реализации шифрования at-rest и in-transit, покрытие типовых требований стандартов, категория остаточного риска, гибкость масштабирования, совокупная стоимость владения и операционная сложность. Для количественного сопоставления использована единая шкала 0–100, значения по которой получены экспертным путём с опорой на публикации [7; 9; 10; 14] и практику реализации информационной безопасности в банках. Оценка угроз выполнялась по шкалам вероятности P и ущерба I со значениями от 1 до 5; интегральный риск $R = P \times I$ использовался для приоритизации мер защиты [7; 9]. Угрозы классифицированы по расширенной модели STRIDE и сопоставлены с перечнем CSA Pandemic Eleven [13].

Количественные оценки получены агрегированием экспертных суждений по четырёхшаговой процедуре: (1) формирование исходного набора критериев на основе NIST SP 800-53 Rev. 5 и ISO/IEC 27001:2022 Annex A; (2) независимая оценка каждого критерия по шкале 0–100 тремя специалистами в области информационной безопасности банков и процессинговых центров; (3) согласование оценок методом скорректированного среднего с отсечением крайних значений; (4) верификация полученных величин по данным публикаций [7; 9; 14] и типовым архитектурным шаблонам. Применение единой процедуры к трём моделям развёртывания обеспечивает сопоставимость результатов и устойчивость выводов относительно порядковой шкалы — различия в оценках между моделями превышают оценочную погрешность и сохраняют знак даже при умеренных вариациях исходных данных.

Сопоставление мер защиты с контролями стандартов выполнялось по прямому соответствию категорий: криптографическая защита — группы A.8.24, A.8.25 (ISO/IEC 27001:2022), семейство SC (System and Communications Protection) и AC (Access Control) в NIST SP 800-53 Rev. 5; управление ключами — A.8.24 и SC-12, SC-13, SC-17; аудит и мониторинг — A.8.15, A.8.16 и семейство AU. Для оценки адекватности мер учитывались требования PCI DSS v4.0 к разделу 3 «Защита хранимых данных держателей карт» и к разделу 4 «Защита данных при передаче» [4]. Результаты такого сопоставления представлены далее в отдельной таблице и позволяют формировать трассировку «архитектурное решение → мера защиты → контроль стандарта», что упрощает последующий аудит.

Архитектура и границы доверия

Типовая архитектура распределённой и облачной системы для финансового сектора включает четыре зоны. Зона клиента — рабочие станции сотрудников, мобильные банковские приложения, веб-браузеры, терминалы самообслуживания; данные здесь формируются и проходят первичную обработку до передачи на периметр. Периметр организации — шлюзы прикладного уровня, балансировщики нагрузки, системы аутентификации и авторизации, межсетевые экраны, веб-экраны прикладного уровня (WAF); здесь проходит первая граница доверия, на которой входящий трафик подвергается инспекции, аутентификации и журналированию. Зона облачного провайдера — виртуальные машины, контейнерные платформы, управляемые сервисы приложений, СУБД, очередей сообщений и хранилищ объектов; на втором рубеже доверия инфраструктура организации сменяется инфраструктурой провайдера, а контроль над гипервизором и физическими узлами переходит к внешней стороне. Зона данных — первичные хранилища, резервные копии, журналы транзакций и аудита; контроль над размещением, криптографической защитой и сроками

хранения данных в этой зоне критичен для соответствия стандартам и требованиям регуляторов [7; 8].

Границы доверия не тождественны сетевым границам. Даже в пределах одной виртуальной сети провайдера обмен между сервисами может пересекать границу доверия, если различаются уровни критичности данных или режимы их обработки. Поэтому современные архитектуры в финансовом секторе всё чаще строятся по принципам zero-trust: любое соединение аутентифицируется и авторизуется независимо от сетевой позиции, применяется mTLS для внутренних вызовов, а политика доступа выражается в явных правилах, связанных с атрибутами идентичности. Такой подход ограничивает возможность горизонтального перемещения злоумышленника в случае компрометации отдельного узла и существенно снижает риск утечки между тенантами в мультитенантной среде [13; 14].

Дополнительным архитектурным рубежом, проходящим внутри облачной зоны, является плоскость управления (control plane) — совокупность API провайдера, порталов администрирования, сервисов IAM и журналов аудита. Компрометация учётных записей администраторов в плоскости управления способна обойти все последующие меры защиты данных, поэтому в современных архитектурах финансового сектора доступ к плоскости управления ограничивается выделенными рабочими местами администраторов, обязательной многофакторной аутентификацией с аппаратными токенами, политикой времени доступа и независимым от провайдера SIEM, в который реплицируются журналы действий. В сочетании с сервисной моделью меши сервисов и шлюзом прикладного уровня, выполняющим централизованную аутентификацию и авторизацию, это позволяет реализовать модель zero-trust в продуктивных развёртываниях без существенного усложнения эксплуатации.

Модель разделённой ответственности уточняет, какие функции защиты выполняет провайдер, а какие остаются за заказчиком, в зависимости от сервисной модели: IaaS, PaaS или SaaS. В IaaS организация отвечает за операционную систему виртуальной машины, прикладные компоненты, данные, управление идентичностью и криптографию; провайдер обеспечивает физическую безопасность, сетевое оборудование и гипервизор. В PaaS организация сосредоточена на коде приложения и данных, тогда как операционная система и runtime становятся зоной ответственности провайдера. В SaaS организация отвечает преимущественно за классификацию данных, управление учётными записями и конфигурацию прикладных настроек, а всё остальное обеспечивает провайдер. Распределение ответственности в долевом выражении приведено на рисунке 1. Пренебрежение формальной фиксацией этой модели в договорных документах и архитектурных регламентах является одной из наиболее частых причин несоответствия аудитам и нарушений SLA по безопасности [3; 11].

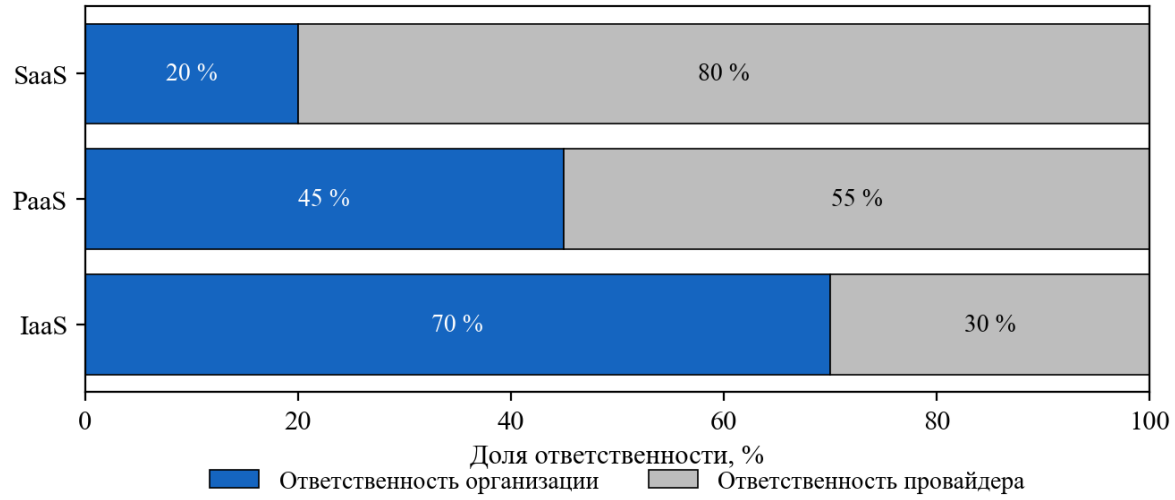

Рисунок 1. Распределение ответственности заказчика и провайдера по сервисным моделям IaaS, PaaS, SaaS

Меры защиты применяются на каждой границе: шифрование при передаче (TLS 1.2/1.3, mTLS, VPN IPsec), шифрование при хранении (at-rest), управление ключами в специализированных сервисах (KMS — Key Management Service; HSM — Hardware Security Module, сертифицированных по FIPS 140-2/3), сегментация сети, строгое разграничение прав в плоскости управления, независимый аудит действий администраторов. На рисунке 2 приведена линейчатая диаграмма оценки риска R = P × I по пяти ключевым угрозам в распределённых и облачных системах; наибольшие значения соответствуют несанкционированному доступу к данным в облаке и компрометации ключей, находящихся в KMS провайдера.

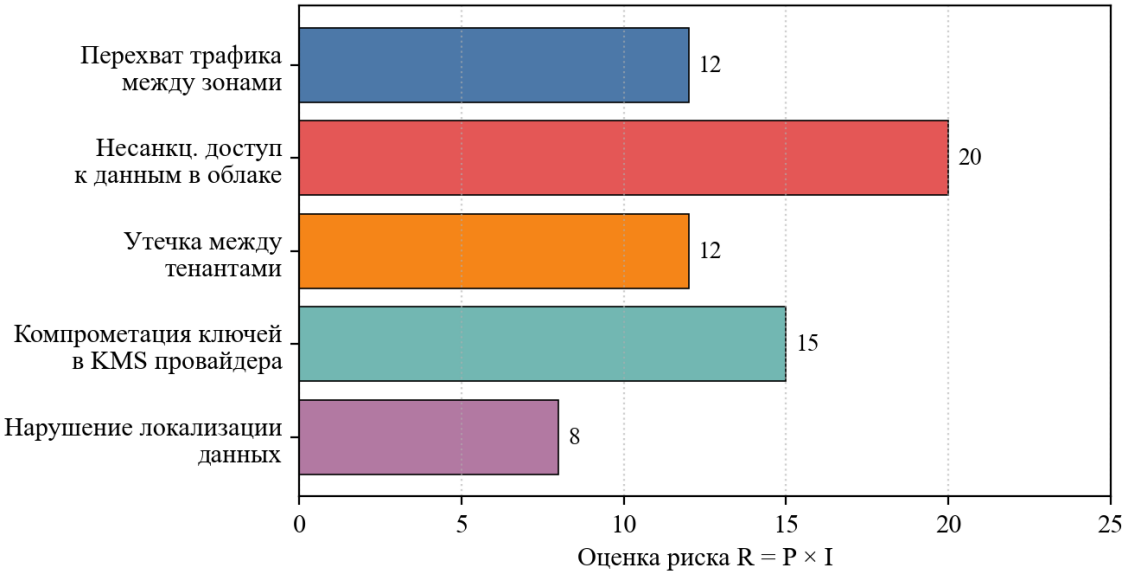

Рисунок 2. Оценка риска R = P × I по типам угроз в распределённых и облачных системах

Угрозы и меры защиты

В распределённых и облачных системах к традиционным угрозам — вредоносному программному обеспечению, атакам отказа в обслуживании, перехвату трафика и инсайдерским злоупотреблениям — добавляются угрозы, специфичные для мультитенантной модели и передачи части контроля провайдеру. Среди них: утечка данных между тенантами в результате уязвимостей в гипервизоре или общих сервисах; неправомерный доступ персонала провайдера к данным заказчика; компрометация ключей, хранящихся в штатном KMS провайдера; несоответствие фактического географического размещения данных договорным и регуляторным требованиям; недостаточная изоляция резервных копий и журналов аудита; конфигурационные ошибки при описании политик доступа к облачным ресурсам и ошибки IAM [9; 10; 13; 14].

Дополнительный класс угроз связан с ошибками и непредсказуемостью поведения сторонних сервисов, интегрируемых в финансовые приложения (платёжные шлюзы, сервисы идентификации, биометрии, антифрод-модули). При выносе части функций к внешним провайдерам часть пользовательских и транзакционных данных пересекает несколько границ доверия, а цепочка ответственности становится многозвенной. Нарушение конфиденциальности на одном из звеньев способно повлечь за собой каскадные последствия для всей цепочки, даже если непосредственный заказчик реализовал все требования стандартов в собственном контуре. Минимизация риска достигается заключением соглашений об уровне защиты (Data Processing Agreement), проведением регулярных оценок поставщиков и применением сквозного шифрования, при котором промежуточные звенья не получают доступ к данным в открытом виде.

Для классификации угроз использована расширенная модель STRIDE, сопоставленная с категориями отчёта CSA «Top Threats to Cloud Computing — Pandemic Eleven» (2022). Наибольшие значения интегрального риска $R = P \times I$ получают угрозы, связанные с раскрытием информации (information disclosure) и подменой субъекта (spoofing), поскольку в финансовом секторе ущерб от утечки клиентских и платёжных данных имеет как прямое финансовое, так и репутационное выражение, а вероятность реализации этих угроз при слабом управлении ключами остаётся высокой. Угрозы отказа в обслуживании, напротив, характеризуются высоким ущербом, но при наличии эластичного масштабирования и защит уровня провайдера — умеренной вероятностью в типовом развёртывании финтех-продукта [10; 14].

В таблице 1 приведены основные угрозы, зоны возникновения, затрагиваемые характеристики безопасности и рекомендуемые меры защиты, а в таблице 2 — реестр рисков с конкретными значениями вероятности P, ущерба I и интегральной оценки R, использованными для построения рисунка 2.

Таблица 1. Угрозы в распределённых и облачных системах и рекомендуемые меры

Угроза	Зона	Затрагиваемая характеристика	Рекомендуемая мера
Перехват трафика между клиентом и облаком	Периметр, каналы	Конфиденциальность	TLS 1.3, mTLS между сервисами, HSTS, pinning

Несанкционированный доступ к данным в облаке	Облако, данные	Конфиденциальность, целостность	Шифрование at-rest с BYOK, RBAC, сегментация, мониторинг
Утечка данных между тенантами	Облако	Конфиденциальность	Криптографическая изоляция, выделенные экземпляры, отдельные ключи
Компрометация ключей в KMS провайдера	Облако	Конфиденциальность, целостность	Собственный KMS/HSM, BYOK или HYOK, ротация ключей, envelope encryption
Нарушение требований к локализации данных	Данные	Соответствие	Выбор региона размещения, договорные гарантии, шифрование с локальными ключами
Инсайдерская угроза со стороны персонала провайдера	Облако, данные	Конфиденциальность	Разделение ключей (SoD), аудит привилегированного доступа
Ошибки конфигурации IAM и публичный доступ к хранилищам	Облако	Конфиденциальность, целостность	IaC-проверки, CSPM, принцип наименьших привилегий, запрет публичных ACL

Из таблицы 1 видно, что меры защиты должны охватывать каналы передачи (TLS, mTLS, VPN), хранилища (шифрование at-rest с контролем над ключами), плоскость управления (строгий IAM, мониторинг привилегированных действий) и организационные аспекты (локализация, договорные обязательства, процедуры реагирования на инциденты). Максимальное снижение риска дают шифрование при хранении с ключами под контролем организации (BYOK — Bring Your Own Key) и строгое разграничение доступа по принципу наименьших привилегий. Для мультитенантной среды критична криптографическая изоляция — выделение отдельных ключей шифрования для каждого тенанта, а при обработке особо чувствительных данных — использование выделенных экземпляров сервисов или аппаратно изолированных анклавов (confidential computing).

Таблица 2. Реестр рисков: оценки вероятности P, ущерба I и интегрального риска R

№	Угроза	P (1–5)	I (1–5)	R = P × I	Категория
1	Перехват трафика между зонами	3	4	12	Средний
2	Несанкционированный доступ к данным в облаке	4	5	20	Высокий
3	Утечка данных между тенантами	3	4	12	Средний
4	Компрометация ключей в KMS провайдера	3	5	15	Средний/высокий
5	Нарушение локализации данных	2	4	8	Умеренный
6	Инсайдерская угроза со стороны персонала провайдера	2	5	10	Средний
7	Ошибки конфигурации IAM и хранилищ	4	4	16	Высокий

Для расчёта интегрального риска в таблице 2 использованы средние экспертные оценки вероятности и ущерба, полученные по той же четырёхшаговой процедуре, что и оценки моделей развёртывания в предыдущем разделе. Диапазон значений R = P × I варьируется от 1 до 25; на практике в программе управления рисками финансовой организации пороговые значения адаптируются к профилю деятельности: для банков с большой долей розничных

платежей порог перехода в категорию «высокий» обычно снижается до $R \geq 12$, поскольку массовые инциденты с клиентскими данными порождают непропорционально высокий репутационный ущерб. В настоящей работе сохранён консервативный порог $R \geq 15$ как общий ориентир, позволяющий сопоставлять оценки между различными типами организаций.

Анализ публично раскрытых инцидентов в облачных развёртываниях финансовых и смежных организаций позволяет выделить три повторяющихся сценария. Первый сценарий — неправильно настроенные политики доступа к объектным хранилищам, при которых резервные копии баз данных или журналы транзакций оказываются доступны извне без аутентификации; подобные случаи зафиксированы у ряда глобальных банков и финтех-компаний в 2019–2022 годах и, по совокупным оценкам отраслевых отчётов, формируют до 40 % публично раскрытых утечек в облаке. Второй сценарий — компрометация долгоживущих сервисных учётных записей и API-ключей, случайно сохранённых в репозиториях исходного кода или в образах контейнеров; последствия таких инцидентов усугубляются широкими правами сервисных учётных записей и отсутствием механизма их автоматического обновления. Третий сценарий — атаки через цепочку поставок программного обеспечения, когда скомпрометированная сторонняя зависимость или подменённый образ базового слоя контейнера становится точкой входа в облачную инфраструктуру организации. Каждый из этих сценариев напрямую отображается в меры таблицы 1 и подчёркивает значимость контролей CSPM, управления секретами и подписи артефактов сборки.

Категории «средний» и «высокий» соответствуют значениям $R = 10–14$ и $R \geq 15$. Угрозы с $R \geq 15$ требуют безусловного применения базового набора мер и регулярной повторной оценки, поскольку даже единичная реализация такой угрозы способна привести к нарушению тайны банковских операций и значительному регуляторному ущербу. Угрозы с $R = 8–14$ закрываются комбинацией технических и организационных мер, приведённых в таблице 1, и включаются в программу планового аудита. Такой подход соответствует методике, изложенной в NIST SP 800-30 Rev. 1 и на которую ссылается NIST SP 800-144 применительно к облачным развёртываниям.

Шифрование и управление ключами по зонам

Шифрование при передаче (in-transit) обеспечивается на каждой границе доверия. На участке клиент–периметр используется TLS версии 1.2 или 1.3 с набором алгоритмов, включающим AES-GCM или ChaCha20-Poly1305 и эфемерный обмен ключами по схеме ECDHE, что гарантирует forward secrecy. На участке периметр–облако применяются TLS-туннели, а при подключении локального ЦОД к облачному провайдеру — IPsec VPN или выделенные защищённые каналы. Для обмена между сервисами внутри облачного развёртывания рекомендуется mTLS (взаимный TLS), при котором обе стороны соединения аутентифицируются сертификатами, выпущенными корпоративным удостоверяющим центром; такая схема является одним из базовых элементов архитектуры zero-trust и упрощает построение межсервисных политик доступа. Конфигурация веб-сервера для принуждения TLS 1.3 может задаваться следующим фрагментом (псевдокод):

TLSProtocol = 1.3; TLSCipherSuites = TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256; HSTS max-age = 31536000; includeSubDomains.

Шифрование при хранении (at-rest) применяется к дискам виртуальных машин, данным в управляемых СУБД, объектным хранилищам и резервным копиям. Базовый алгоритм — AES-256 в режиме GCM или XTS; для СУБД используется прозрачное шифрование (Transparent Data Encryption, TDE), для файловых систем — LUKS или эквивалентные механизмы, для объектных хранилищ — серверное шифрование с ключами, которыми управляет заказчик. Критическим вопросом является владение ключами. При использовании встроенного KMS провайдера (SSE-S3, provider-managed keys и их аналоги) ключи технически могут быть доступны провайдеру, что для финансового сектора не всегда приемлемо. Модель BYOK (Bring Your Own Key) предполагает генерацию мастер-ключа в инфраструктуре заказчика и импорт его в KMS провайдера, модель HYOK (Hold Your Own Key) — хранение ключей исключительно на стороне заказчика, а криптографические операции при этом выполняются либо на стороне клиента, либо через защищённый канал к внешнему HSM.

Практика ротации ключей в развёртываниях финансовых организаций опирается на сочетание плановых и событийно-инициируемых процедур. Плановая ротация DEK выполняется по расписанию (типично — ежемесячно или ежеквартально для систем с высокой частотой обновления данных), ротация KEK — ежегодно или с периодичностью, согласованной с жизненным циклом сертификатов удостоверяющего центра. Событийная ротация инициируется при компрометации учётных данных, увольнении администратора с привилегированным доступом, изменении состава персонала провайдера или при выявлении уязвимостей в используемой криптографической библиотеке. Процедуры ротации автоматизируются и тестируются в средах предпродуктивной эксплуатации, поскольку ошибочная замена KEK в продуктивной системе без корректного пересечного перешифрования DEK способна сделать данные временно или постоянно недоступными. Резервное копирование самих ключей осуществляется в изолированную среду с мультиличностным контролем доступа и логированием каждой операции восстановления.

В промышленных развёртываниях применяется иерархическое шифрование (envelope encryption): данные зашифрованы ключом данных (DEK — Data Encryption Key), а сам DEK зашифрован ключом шифрования ключей (KEK — Key Encryption Key), который хранится в KMS или HSM. Такая схема позволяет быстро сменить ключ верхнего уровня без перешифрования всего объёма данных и реализует механизм криптошреддинга (crypto-shredding): уничтожение ключа верхнего уровня делает зашифрованные данные безвозвратно нечитаемыми, что важно как для процедур удаления, так и для соблюдения сроков хранения. Периодичность ротации ключей определяется политикой организации и рекомендациями NIST SP 800-57 Part 1 Rev. 5: для KEK характерны интервалы в 1–2 года, для DEK — значительно меньшие, вплоть до ротации при каждой операции записи в чувствительные хранилища. HSM, используемые для хранения корневых ключей, должны быть сертифицированы как минимум по FIPS 140-2 уровня 3 или по соответствующему уровню FIPS 140-3, а доступ к ним регулироваться по принципу разделения обязанностей (SoD) и двойного контроля [5; 11; 12].

Для данных платёжных карт альтернативой или дополнением к шифрованию выступает токенизация — замена чувствительного значения (номера карты, PAN) на суррогатное, не

имеющее криптографической связи с оригиналом. Токенизация, выполняемая в собственном токен-вейлте организации, исключает хранение PAN в облачных сервисах, сужает область действия PCI DSS и упрощает последующий аудит. В сочетании с шифрованием at-rest и политикой вывода PAN из облачной зоны токенизация позволяет достичь уровня остаточного риска, сопоставимого с собственным ЦОД, даже для SaaS-систем фронт-офиса. Для персональных данных клиентов применимы аналогичные подходы — псевдонимизация и ограничение обработки прямых идентификаторов пределами собственного периметра, что согласуется с требованиями статьи 32 GDPR и рекомендациями ENISA.

Сопоставление мер защиты по зонам приведено в таблице 3. Из неё видно, что наилучшее соответствие требованиям стандартов достигается при сохранении контроля над ключами на стороне организации и сочетании криптографической защиты с сегментацией сети, строгим управлением идентичностью и независимым аудитом. На рисунке 3 показано, какой вклад в суммарное снижение риска вносят отдельные меры защиты; наибольший эффект дают шифрование при хранении с управляемыми организацией ключами и разграничение доступа.

Таблица 3. Меры защиты данных по зонам

Зона	Меры	Контроль над ключами	Влияние на соответствие стандартам
Клиент — периметр	TLS 1.3, MFA, сертификат-пиннинг, HSTS	Ключи сессии у клиента и сервера	Защита каналов (ISO 27001 A.8.24, PCI DSS 4)
Периметр — облако	TLS/mTLS, VPN IPsec, выделенные каналы	Организация управляет сертификатами	Изоляция трафика, NIST SC-8, SC-12
Облако (узлы, сервисы)	Шифрование at-rest, RBAC, сегментация	При BYOK/HSM — у организации	Критично для конфиденциальности, A.8.25
Данные (хранилища, бэкапы)	At-rest (AES-256), изолированные копии, crypto-shredding	Рекомендуется ключи у организации	Целостность, восстановление, SC-28

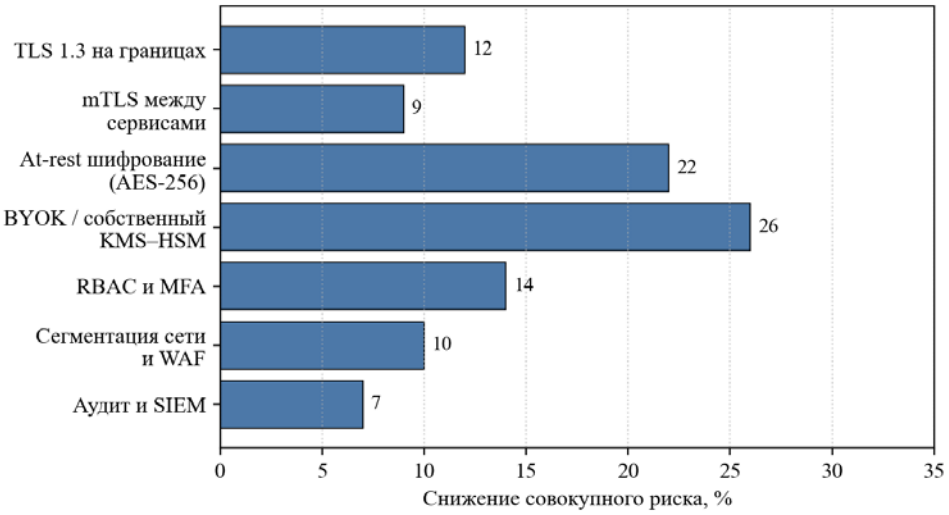

Рисунок 3. Снижение совокупного риска при внедрении отдельных мер защиты, %

Для упрощения аудита и прослеживаемости соответствия архитектурных решений требованиям стандартов в таблице 4 приведено отображение мер защиты на контроли ISO/IEC 27001:2022 (Annex A) и NIST SP 800-53 Rev. 5. Такая таблица-соответствие используется при подготовке к внешним проверкам и внутренним ревизиям, а также при формировании требований в договорах с облачными провайдерами.

Таблица 4. Соответствие мер защиты контролям ISO/IEC 27001:2022 и NIST SP 800-53 Rev. 5

Мера	ISO/IEC 27001:2022 (Annex A)	NIST SP 800-53 Rev. 5	PCI DSS v4.0
TLS 1.2/1.3 и mTLS на каналах	A.8.24, A.8.20	SC-8, SC-13	4.2
Шифрование at-rest (AES-256)	A.8.24, A.8.25	SC-28, SC-13	3.5
BYOK / собственный KMS–HSM	A.8.24	SC-12, SC-17	3.6, 3.7
RBAC, MFA, принцип наименьших привилегий	A.5.15, A.5.18, A.8.2	AC-2, AC-3, AC-6, IA-2	7, 8
Журналирование и SIEM	A.8.15, A.8.16	AU-2, AU-6, AU-12	10
Сегментация сети и WAF	A.8.22, A.8.23	SC-7, SC-32	1
Управление конфигурацией и CSPM	A.8.9, A.8.32	CM-2, CM-6, CM-7	2

Сравнение моделей развёртывания

Сравнение трёх моделей по уровню контроля над ключами, наличию и качеству шифрования at-rest и in-transit, покрытию типовых требований стандартов (в процентах) и категории остаточного риска представлено в таблице 5. Для публичного облака рассмотрены варианты с BYOK и без BYOK, поскольку именно наличие собственного контроля над ключами принципиально изменяет оценку модели по большинству критериев [7; 9].

Таблица 5. Сравнительная оценка моделей развёртывания

Модель	Контроль над ключами	Шифрование at-rest / in-transit	Покрытие требований, %	Остаточный риск
On-premise	Полный (собственный HSM/KMS)	Реализуется организацией	90–94	Низкий
Гибридное облако	Частичный (критичные ключи on-premise)	В облаке по контракту и BYOK	72–78	Средний
Публичное облако (без BYOK)	Ограниченный	Ключи и шифрование у провайдера	58–65	Повышенный
Публичное облако (с BYOK)	Приемлемый	Ключи импортируются из on-premise	65–72	Средний

Значение покрытия для on-premise не достигает 100 %, поскольку полная реализация требований стандартов зависит не только от архитектурного контура, но и от зрелости процессов управления информационной безопасностью, регулярности аудитов и качества исполнения организационных мер. Даже в собственном ЦОД организация сталкивается с

рисками, связанными с инсайдерскими действиями, ошибками конфигурации сетевых устройств и уязвимостями прикладного программного обеспечения. Поэтому сравнение моделей по единственному показателю покрытия требований имеет смысл только в совокупности с оценкой остаточного риска и многокритериальным анализом, представленным далее.

Из таблицы 5 следует, что для финансового сектора модель on-premise обеспечивает наивысшее покрытие требований и наименьший остаточный риск ценой высокой совокупной стоимости владения и ограниченной эластичности. Гибридная модель допустима при вынесении в облако некритичных нагрузок (аналитика, вычислительно-ёмкие пакетные задания, среды разработки и тестирования) с сохранением на собственных мощностях ключей шифрования и чувствительных ядер. Публичное облако для критичных данных требует обязательного использования BYOK или собственного KMS/HSM, а также явно прописанных в договоре условий, касающихся локализации данных, сроков уведомления об инцидентах и процедур доступа персонала провайдера к клиентским данным.

На рисунке 4 приведено покрытие требований стандартов в процентах по четырём вариантам моделей развёртывания. Видно, что переход от on-premise к публичному облаку без BYOK сопровождается снижением покрытия примерно на 30 процентных пунктов, тогда как применение BYOK в публичном облаке возвращает в среднем 6–8 п.п. покрытия, поскольку закрывает критический контроль «управление криптографическими ключами».

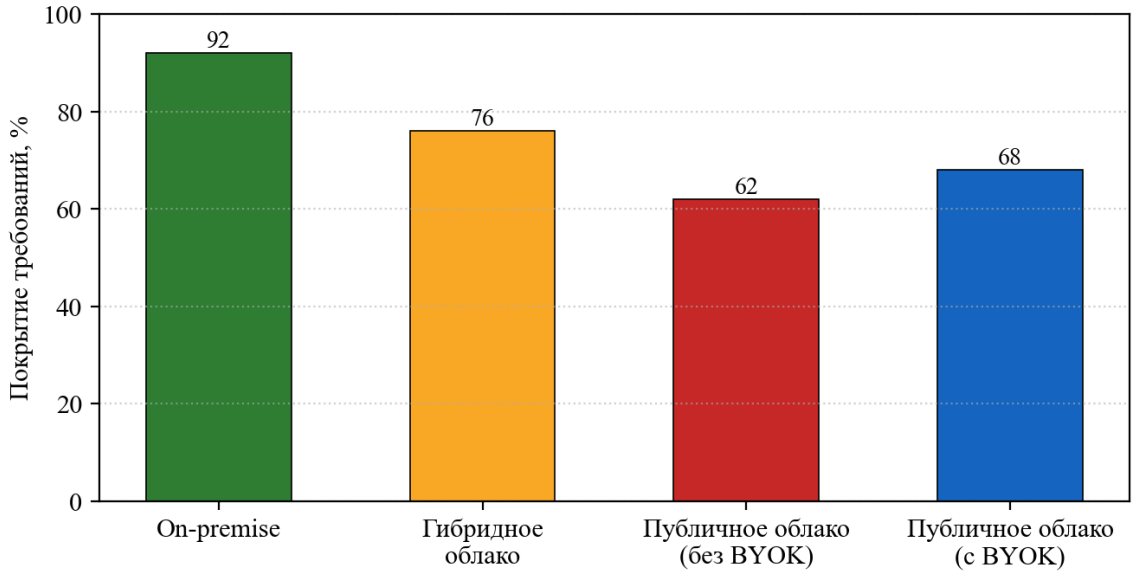

Рисунок 4. Покрытие требований стандартов (%) по моделям развёртывания

Экономическое измерение выбора между моделями не сводится к прямому сопоставлению цены виртуальной машины и стоимости собственного оборудования. В совокупную стоимость владения входят расходы на помещение, инженерные системы, лицензии на программное обеспечение, персонал круглосуточного сопровождения, резервирование по площадкам, процедуры непрерывности бизнеса и восстановления после сбоев. Публичное облако перераспределяет эти статьи в операционные расходы и делает их частью цены потребляемого сервиса, что в ряде сценариев — в особенности для нагрузок с выраженной сезонностью и переменным профилем потребления — обеспечивает экономию в

25–40 % совокупной стоимости владения. Для ядер АБС с постоянной нагрузкой и высокими требованиями к латентности экономический эффект публичного облака снижается, а иногда становится отрицательным, что делает гибридную модель более сбалансированным выбором.

Однако покрытие требований не исчерпывает полной картины. На рисунке 5 приведена многокритериальная оценка трёх моделей развёртывания по пяти параметрам: контроль над ключами, покрытие стандартов, гибкость развёртывания, TCO-эффективность и операционная сложность (для последнего параметра большее значение соответствует меньшей сложности эксплуатации). Модель on-premise устойчиво лидирует по контролю над ключами и покрытию стандартов, но проигрывает по гибкости и совокупной стоимости. Публичное облако с BYOK показывает сбалансированный профиль, обеспечивая приемлемый уровень безопасности при сохранении экономических и операционных преимуществ. Гибрид занимает промежуточное положение и часто оказывается практическим компромиссом для банков, последовательно мигрирующих периферийные нагрузки при сохранении ядра АБС в собственном периметре.

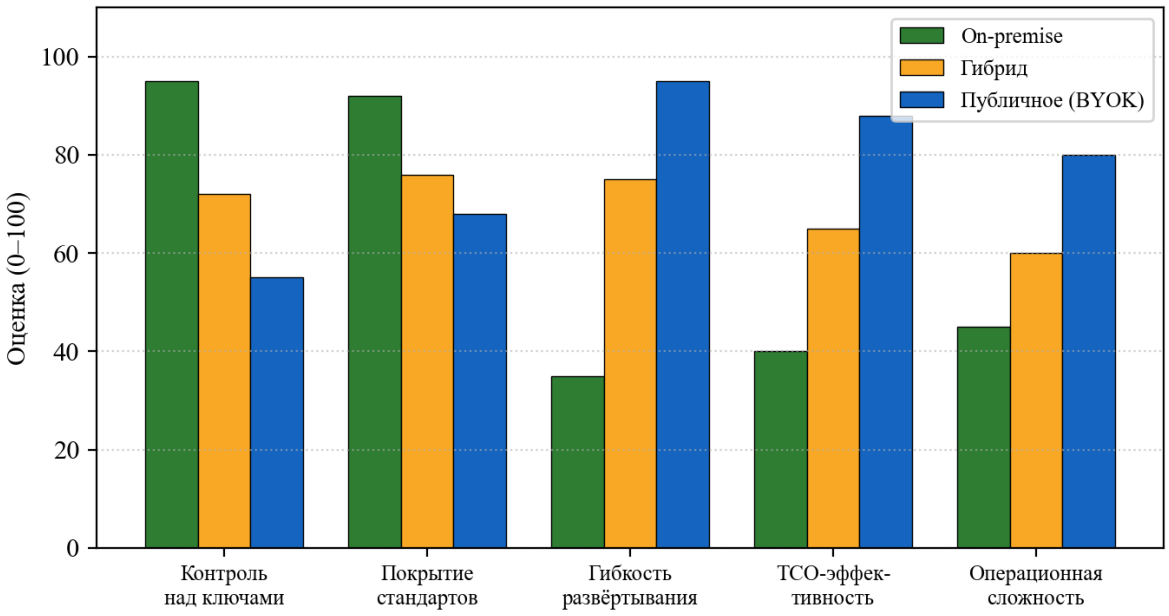

Рисунок 5. Многокритериальная оценка моделей развёртывания

Обсуждение результатов и практические рекомендации

Полученные количественные оценки согласуются с выводами исследований: определяющим фактором приемлемости облачной модели для финансового сектора остаётся контроль над криптографическими ключами. Различия между вариантами публичного облака с BYOK и без BYOK составляют в среднем 6–8 процентных пунктов по покрытию требований и одну-две ступени по категории остаточного риска. Менее очевиден, но существен вклад зрелости процессов управления плоскостью управления облака: ошибки IAM и конфигурационные недочёты, согласно данным CSA, остаются одной из трёх ведущих причин инцидентов в облачных развёртываниях. В практическом смысле это означает, что инвестиции в криптографию без параллельного развития инструментов CSPM и инфраструктуры как кода с автоматической проверкой политик не обеспечивают ожидаемого снижения риска.

На основе проведённого анализа для банков, процессинговых центров и платёжных организаций могут быть предложены следующие практические рекомендации. Во-первых, формализовать модель разделённой ответственности в архитектурной документации и договорах с провайдером, с явным перечнем контролей, закреплённых за каждой стороной, и процедурой реагирования на инциденты. Во-вторых, реализовать шифрование при хранении с BYOK или собственным HSM для всех систем, обрабатывающих данные держателей карт, персональные данные клиентов и сведения, составляющие банковскую тайну. В-третьих, использовать envelope encryption и выделенные ключи для каждого тенанта, а для процедур удаления — механизм криптошреддинга, позволяющий гарантированно прекратить доступ к архивным данным. В-четвёртых, применять подход zero-trust во внутренних коммуникациях, включая mTLS и политику наименьших привилегий, а плоскость управления облака защищать обязательной MFA, журналированием привилегированных действий и независимым от провайдера аудитом.

Полученные результаты применимы и к процессам непрерывности бизнеса. Для распределённых развёртываний ключевым показателем становится не просто время восстановления сервиса (RTO), а возможность сохранить контроль над ключами шифрования при отказе основного региона. Практической реализацией этого требования является двухконтурная схема управления ключами: рабочий контур в регионе основной эксплуатации и резервный контур в собственном ЦОД или во втором регионе, синхронизируемый через безопасный канал. Даже при полном отказе основного облачного региона организация сохраняет способность расшифровать резервные копии и продолжить операции на альтернативной площадке без обращения к провайдеру за восстановлением ключей. Такой подход снимает один из классических возражений против публичного облака и делает его применимым для систем с высокими требованиями по непрерывности.

В-пятых, выстроить процесс непрерывного мониторинга соответствия конфигурации требованиям с помощью инструментов CSPM и IaC-сканеров, интегрированных в конвейер CI/CD; в-шестых, регулярно проводить оценку рисков по методике, совместимой с NIST SP 800-30 и ISO/IEC 27005, с обязательным пересмотром реестра рисков при каждой существенной архитектурной изменении. В-седьмых, в гибридных и публичных развёртываниях включать в договор с провайдером условия о локализации данных, ограничении доступа персонала провайдера и сроках уведомления о выявленных инцидентах (не более 24–72 часов в зависимости от критичности). Последовательное применение этих рекомендаций позволяет снизить остаточный риск в публичном облаке с BYOK до уровня, сопоставимого с гибридной моделью, а для некритичных нагрузок — сделать публичное облако безопасной и экономически эффективной альтернативой собственному ЦОД.

Отдельного внимания заслуживает направление конфиденциальных вычислений (confidential computing), основанное на аппаратных доверенных средах исполнения (TEE): Intel SGX/TDX, AMD SEV-SNP, ARM CCA. Технология TEE обеспечивает шифрование оперативной памяти виртуальной машины и её изоляцию от гипервизора и администраторов провайдера, что принципиально сокращает поверхность атаки со стороны инфраструктурного уровня и делает допустимой обработку зашифрованных данных в открытом виде внутри анклава без раскрытия ключей провайдеру. Для финансового сектора TEE рассматривается как механизм защиты критичных вычислений — моделей скоринга, аналитики транзакций, процедур KYC/AML — в публичном облаке. Практическая применимость технологии

ограничивается зрелостью экосистемы и требует аттестации анклавов (remote attestation), согласованных с политиками организации процедур, а также учёта изменений в модели угроз при переходе от программной к аппаратной изоляции.

Ограничения исследования связаны с экспертным характером количественных оценок и их зависимостью от конкретного провайдера, региона размещения и зрелости процессов заказчика. Для отдельных сценариев (платёжные шлюзы, системы мгновенных переводов, core banking) распределение процентов может отличаться на 5–10 п.п. в ту или иную сторону. Тем не менее предложенная методика (четыре зоны защиты, реестр рисков с шкалами P и I, таблица соответствия мер стандартам, многокритериальная оценка моделей) инвариантна к этим изменениям и может быть применена как шаблон в проектных работах по архитектуре информационной безопасности.

Заключение

В работе систематизированы подходы к защите данных в распределённых и облачных серверных системах применительно к финансовому сектору. Построена модель зон защиты и границ доверия, сформированы таблицы угроз и мер защиты по зонам, составлен реестр рисков с конкретными значениями вероятности и ущерба, выполнено отображение мер на контроли ISO/IEC 27001:2022 и NIST SP 800-53 Rev. 5, проведено количественное сравнение трёх моделей развёртывания. Установлено, что ключевыми факторами соответствия стандартам и снижения риска являются сохранение контроля над ключами шифрования, применение шифрования при хранении и при передаче во всех зонах, явное распределение ответственности с провайдером, зрелость процессов управления плоскостью управления облака и непрерывный контроль конфигурации.

Полученные количественные ориентиры могут использоваться как базовые значения в проектных работах и в обосновании архитектурных решений перед руководством и регулятором. Приведённый реестр рисков с оценками $R = P \times I$ позволяет приоритизировать меры защиты даже при ограниченных ресурсах, направляя их в первую очередь на закрытие угроз с $R \geq 15$. Таблица соответствия мер защиты контролям ISO/IEC 27001:2022 и NIST SP 800-53 Rev. 5 упрощает подготовку к аудитам и сокращает цикл согласования с внутренними и внешними проверяющими.

Практическая ценность результатов состоит в применимости предложенной методики и количественных ориентиров при принятии решений о переносе систем в облако и при проектировании архитектуры защиты в банках, процессинговых центрах и платёжных организациях. Перспективы развития работы — детализация требований к аудиту облачных провайдеров, расширение сравнения на отраслевые сценарии, изучение применимости confidential computing и полностью гомоморфного шифрования для обработки чувствительных финансовых данных в недоверенных средах, а также адаптация предложенной методики к условиям финансовых организаций Кыргызской Республики с учётом требований Национального банка.

Список литературы

1. Алыбаев К. К., Токтосунов А. А. Вопросы информационной безопасности в облачных сервисах // Вестник ОшГУ. 2020. № 2. С. 45–51.
2. Оморов М. С., Ибраимова Г. К. Защита данных в распределённых информационных системах // Наука, новые технологии и инновации Кыргызстана. 2019. № 4. С. 78–82.
3. Аркабаев, Н., & Алымова, З. (2024). Разработка web серверных приложений на базе .NET Core в примере интернет-магазина. Вестник Ошского государственного университета, (1), 142–154. https://doi.org/10.52754/16948610_2024_1_13
4. Омаралиев, А., Карабаев, С., Омаралиева, Г., & Вэньхао, Д. (2025). Методология тестирования безопасности веб-приложений на Django с акцентом на выявление уязвимостей бизнес-логики. Вестник Ошского государственного университета, (4), 199–211. https://doi.org/10.52754/16948610_2025_4_14
5. Белов Е. Б., Лось В. П. Основы информационной безопасности. М.: Горячая линия-Телеком, 2020. 544 с.
6. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. М.: ИД «Форум»: Инфра-М, 2019. 416 с.
7. Смирнов С. Н., Кузнецов А. В. Управление ключами шифрования в гибридных облачных средах // Прикладная информатика. 2021. Т. 16. № 3. С. 45–56.
8. Федоров А. И., Петрова О. В. Защита персональных данных в облачных сервисах финансового сектора // Информационная безопасность. 2022. Т. 19. № 2. С. 88–95.
9. Hashizume K., Rosado D. G., Fernández-Medina E., Fernandez E. B. An analysis of security issues for cloud computing // Journal of Internet Services and Applications. 2013. Vol. 4. No. 1. P. 1–13.
10. Fernandes D. A. B., Soares L. F. B., Gomes J. V., Freire M. M., Inácio P. R. M. Security issues in cloud environments: a survey // International Journal of Information Security. 2014. Vol. 13. No. 2. P. 113–170.
11. Kaufman L. M. Data security in the world of cloud computing // IEEE Security and Privacy. 2009. Vol. 7. No. 4. P. 61–64.
12. Mell P., Grance T. The NIST Definition of Cloud Computing: NIST Special Publication 800-145. Gaithersburg: NIST, 2011. 7 p.
13. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing: NIST Special Publication 800-144. Gaithersburg: NIST, 2011. 80 p.
14. Cloud Security Alliance. Top Threats to Cloud Computing: Pandemic Eleven. CSA, 2022. 52 p.
15. Subashini S., Kavitha V. A survey on security issues in service delivery models of cloud computing // Journal of Network and Computer Applications. 2011. Vol. 34. No. 1. P. 1–11.
16. Popović K., Hocenski Ž. Cloud computing security issues and challenges // Proceedings of the 33rd International Convention MIPRO. Opatija: IEEE, 2010. P. 344–349.

Евразия изилдөөлөрү ачык журналы, 2026, №3, бб. 110-128
doi: 10.65469/eijournal.2026.3.12
eijournal.ilimbilim.kg

ИНФОРМАТИКА / COMPUTER SCIENCE
УДК 004.056

Бөлүштүрүлгөн жана булуттук сервердик системаларындагы маалыматтарды коргоо (финансы сектору үчүн)

Омаралиева Гулбайра Абдималиковна
Ош мамлекеттик университети, Кыргызстан, gulya@oshsu.kg, ORCID: 0000-0003-1862-2142

Мамасалиев Ажибек Арзиматович
Ош мамлекеттик университети, Кыргызстан, azhibekmamasaliev@gmail.com, ORCID: 0009-0004-9159-4357

Абдыкадыров Султанбек Каныбекович
Ош мамлекеттик университети, Кыргызстан, sultanbekabdykadyrov69@gmail.com, ORCID: 0009-0001-7078-4686

Аннотация
Финансы секторунун уюмдары масштабдуулук, катага туруктуулук жана рынокко чыгуу ылдамдыгы талаптарынан улам сервер системаларын таратылган жана булут чөйрөлөрүнө барган сайын көбүрөөк көчүрүп жатышат. Маалыматтарды өз периметринен тышкары иштетүү купуялуулукка жана бүтүндүккө коркунуч келтирет, провайдерге көз карандылыкты жогорулатат жана ишеним чектерин жана шифрлөө ачкычтарын башкарууну так эске алууну талап кылат. Бул аспектилерди жетишсиз эске алуу инциденттерге, банк купуялуулугунун бузулушуна жана тармактык стандарттарга шайкеш келбегендикке алып келет.

Ачкыч сөздөр: маалыматтарды коргоо, бөлүштүрүлгөн системалар, булуттук эсептөө, ишеним чек аралары, KMS, HSM, BYOK, көп ижаралык, маалыматтык коопсуздук

Open Journal of Eurasian Issues, 2026, no. 3, pp. 110-128
doi: 10.65469/eijournal.2026.3.12
eijournal.ilimbilim.kg

ИНФОРМАТИКА / COMPUTER SCIENCE
УДК 004.056

Data Protection in Distributed and Cloud Server Systems (Case of the Financial Sector)

Gulbaira Abdimalikovna Omaralieva
Osh State University, Kyrgyzstan, gulya@oshsu.kg, ORCID: 0000-0003-1862-2142

Azhibek Arzimatovich Mamasaliev
Osh State University, Kyrgyzstan, azhibekmamasaliev@gmail.com, ORCID: 0009-0004-9159-4357

Sultanbek Kanybekovich Abdykadyrov
Osh State University, Kyrgyzstan, sultanbekabdykadyrov69@gmail.com, ORCID: 0009-0001-7078-4686

Abstract
Financial sector organizations increasingly move server systems to distributed and cloud environments, driven by the need for scalability, resilience, and faster time-to-market. Processing data outside the organization's perimeter creates risks to confidentiality and integrity, increases dependence on the provider, and requires explicit consideration of trust boundaries and encryption key management. Insufficient attention to these aspects leads to incidents, breaches of banking secrecy, and non-compliance with industry standards.

Keywords: data protection, distributed systems, cloud computing, trust boundaries, KMS, HSM, BYOK, multi-tenancy, information security