Ссылка для цитирования этой статьи:

Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Компьютерная безопасность в облачных информационных системах: риски и способы их минимизации // Human Progress. 2024. Том 10, Вып. 6. URL: http://progress-human.com/images/2024/Tom10_6/Solodovnikov.pdf DOI 10.46320/2073-4506-2024-6a-3.

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ: РИСКИ И СПОСОБЫ ИХ МИНИМИЗАЦИИ

Солодовников Дмитрий Викторович
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

Соколов Александр Кириллович
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

Шорохов Константин Дмитриевич
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

Кучук Максим Игоревич
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

Аннотация. В статье рассматриваются современные инновационные подходы к обеспечению безопасности данных в облачных информационных системах. Объект исследования – национальная безопасность. Предмет исследования – экономика компьютерной безопасности. Цель исследования – раскрыть содержание компьютерной безопасности в облачных информационных системах с экономических и технических аспектов. Анализируются технологии, такие как искусственный интеллект, машинное обучение, гомоморфное шифрование, блокчейн и конфиденциальные вычисления, которые обеспечивают повышенный уровень защиты данных и минимизацию рисков. Принцип «нулевого доверия» (Zero Trust) и использование декларативных моделей безопасности также обсуждаются как ключевые стратегии для обеспечения надежности и устойчивости облачных инфраструктур. Описываются примеры их успешного применения в корпоративных облачных системах и преимущества перед традиционными методами защиты данных. Рассматриваемые инновации позволяют значительно повысить безопасность обработки и хранения конфиденциальной информации в условиях современных киберугроз.

DOI 10.46320/2073-4506-2024-6a-3

Ключевые слова: облачные информационные системы, безопасность данных, искусственный интеллект, машинное обучение, гомоморфное шифрование, блокчейн, конфиденциальные вычисления, нулевое доверие, защита данных, кибербезопасность.

Введение

Взаимосвязь между экономикой и кибербезопасностью можно рассматривать с двух ключевых сторон: во-первых, необходимо учитывать экономические последствия кибератак, так как киберугрозы могут привести к значительным финансовым потерям для финансовых институтов, а также к снижению доверия к финансовым системам в целом, что, в свою очередь, может привести к сокращению инвестиций, росту инфляции и другим негативным последствиям для экономики. Во-вторых, необходимо признать влияние кибербезопасности на экономический рост -кибербезопасность является важным фактором для устойчивого экономического развития, а наличие надежных киберсистем обеспечивает стабильность финансовых систем и создает благоприятные условия для инвестиций и инноваций. Угрозы безопасности в облачных информационных системах представляют собой одну из ключевых проблем современной информационной безопасности. Переход на облачные технологии, с одной стороны, предоставляет значительные преимущества в плане гибкости и масштабируемости, но с другой — открывает новые уязвимости для киберугроз. Среди таких угроз стоит выделить утечку данных, атаки на конфиденциальность, DDoS-атаки, неавторизованный доступ и внутренние угрозы. Эти аспекты требуют серьезного внимания и применения современных методов защиты, основанных на криптографии, аутентификации, мониторинге и других технологических решениях.

Основная часть

Одной из ключевых угроз является утечка данных, особенно в многопользовательских облачных средах, где один физический сервер может обслуживать множество организаций. Это создает риск, что данные одного пользователя могут быть случайно или намеренно скомпрометированы другими пользователями или злоумышленниками. Например, в случае с компанией Capital One в 2019 году, утечка данных из облака Amazon Web Services привела к компрометации более 100 миллионов записей клиентов. Основной уязвимостью была ошибка конфигурации, которая позволила злоумышленнику получить доступ к критически важной информации. Этот случай показал, что одна из наиболее значительных проблем облачных систем — неправильная настройка сервисов, что подчеркивает необходимость тщательной проверки и регулярного аудита конфигураций безопасности.

DOI 10.46320/2073-4506-2024-6a-3

Атаки на конфиденциальность данных также являются одной из главных проблем. Поскольку облачные информационные системы хранят огромные объемы персональных данных, они представляют собой привлекательную цель для хакеров, стремящихся получить доступ к информации, такой как номера кредитных карт, медицинские данные и другие конфиденциальные данные [3]. Один из методов защиты, широко используемый для минимизации риска утечки конфиденциальных данных, заключается в применении криптографии. Шифрование данных как при их передаче, так и при хранении стало стандартом для большинства облачных провайдеров. Согласно отчету компании McAfee, к 2023 году более 80% облачных поставщиков применяют шифрование данных "на месте" и "в пути", что значительно снижает вероятность их компрометации даже при взломе системы. Однако на практике криптографические методы не всегда решают проблему, если ключи шифрования хранятся ненадежно или передаются между различными узлами без должной защиты.

DDoS-атаки (Distributed Denial of Service) представляют собой еще одну серьезную угрозу для облачных систем. Эти атаки направлены на перегрузку облачных ресурсов, что делает сервисы недоступными для легитимных пользователей. Увеличение числа таких атак связано с распространением облачных сервисов, которые предоставляют огромные вычислительные мощности и инфраструктурные ресурсы. Согласно отчету компании Netscout, количество DDoS-атак в 2023 году выросло на 16% по сравнению с предыдущим годом, и большая часть этих атак была направлена на облачные системы. Результаты исследований показывают, что использование облачных платформ с механизмами автошкалирования (auto-scaling) может временно смягчить влияние DDoS-атак, увеличивая вычислительные мощности при необходимости, но это решение не является полной защитой, поскольку такие атаки могут значительно увеличить затраты на инфраструктуру и вывести систему из строя при истощении ресурсов.

Неавторизованный доступ к данным в облачных системах также остается одной из главных проблем. Большая часть инцидентов безопасности, связанных с утечками данных, происходит из-за слабых паролей или отсутствия многофакторной аутентификации. Исследование, проведенное Verizon в 2023 году, показало, что около 81% утечек данных связаны с неправильно настроенными механизмами аутентификации и управления доступом. Для предотвращения таких инцидентов широко применяются методы многофакторной аутентификации, а также биометрические системы, которые существенно снижают вероятность несанкционированного доступа. Например, в 2023 году компания Google заявила, что переход на двухфакторную аутентификацию для всех корпоративных пользователей

DOI 10.46320/2073-4506-2024-6a-3

позволил сократить количество неавторизованных попыток доступа на 50%, что свидетельствует о значительном увеличении уровня защиты при использовании данного метода [1].

Кроме внешних угроз, важную роль играют и внутренние угрозы — те, которые исходят от сотрудников организаций или третьих сторон, имеющих легитимный доступ к облачным системам. Согласно данным исследования компании Gartner, в 2023 году 34% всех утечек данных в облачных системах были связаны с внутренними угрозами. Эти инциденты могут быть вызваны как намеренными действиями, так и случайными ошибками сотрудников. Применение строгих политик доступа и регулярный аудит действий сотрудников позволяют снизить риск возникновения таких инцидентов. Например, внедрение политики «минимально необходимых прав» (least privilege), при которой каждому пользователю предоставляется только тот объем доступа, который необходим для выполнения его задач, показало свою эффективность в ряде крупных организаций, таких как Microsoft и IBM, где такие подходы применяются для защиты облачной инфраструктуры.

Для защиты от внутренних угроз также активно используются системы мониторинга и обнаружения аномалий. Эти системы основаны на применении машинного обучения, которое анализирует поведение пользователей и выявляет подозрительную активность. Например, компания Splunk разработала облачную платформу мониторинга, которая использует алгоритмы машинного обучения для обнаружения необычных действий в сети. В 2022 году эта система позволила обнаружить и предотвратить несколько попыток кибератак на корпоративные сети, что подтверждает важность использования передовых технологий для повышения уровня безопасности.

Для минимизации рисков, связанных с угрозами безопасности в облачных информационных системах, активно применяются различные технологические решения, которые направлены на защиту данных, управление доступом, мониторинг и обнаружение угроз, а также на создание более безопасных и устойчивых инфраструктур. Эти решения не только снижают вероятность утечек данных и атак, но и минимизируют потенциальные финансовые потери и урон для репутации организаций.

Одним из ключевых решений для минимизации рисков является шифрование данных. Шифрование позволяет защитить информацию как на этапе хранения, так и во время передачи между клиентом и облачными серверами. Современные облачные провайдеры, такие как Amazon Web Services (AWS), Microsoft Azure и Google Cloud, предлагают комплексные решения для шифрования данных на стороне клиента и на сервере [4]. В 2023 году более 85% облачных сервисов использовали шифрование данных в процессе хранения и передачи, что

DOI 10.46320/2073-4506-2024-6a-3

значительно снижает вероятность утечки данных даже в случае взлома облачной инфраструктуры. Важным компонентом этого процесса является управление ключами шифрования. Использование технологий, таких как AWS Key Management Service (KMS) или Azure Key Vault, позволяет централизованно управлять ключами и обеспечивать их надежное хранение, предотвращая несанкционированный доступ.

Важной составляющей обеспечения безопасности является многофакторная аутентификация (MFA). MFA позволяет защитить доступ к облачным системам с помощью дополнительных факторов, таких как временные пароли или биометрические данные, что снижает риски, связанные с компрометацией учетных записей. Внедрение многофакторной аутентификации широко признано как один из самых эффективных методов защиты облачных систем от неавторизованного доступа. Например, согласно отчету Google, переход на обязательное использование двухфакторной аутентификации среди корпоративных клиентов в 2023 году снизил количество несанкционированных попыток входа более чем на 90%. Это особенно важно в условиях постоянного увеличения числа фишинговых атак и попыток перехвата учетных данных.

Помимо методов аутентификации, важным элементом является управление правами доступа (Identity and Access Management, IAM). Системы IAM обеспечивают контроль за тем, кто и к каким ресурсам облака имеет доступ, на основании ролей и полномочий. Современные системы IAM, такие как Microsoft Azure Active Directory или AWS IAM, предоставляют возможность управлять доступом к ресурсам на уровне отдельных пользователей и групп, что позволяет гибко регулировать уровень прав доступа. Например, внедрение политики «минимально необходимых прав» (least privilege) позволяет минимизировать вероятность ошибок или злонамеренных действий сотрудников, предоставляя им доступ только к тем ресурсам, которые необходимы для выполнения их задач. Согласно исследованию компании Gartner, внедрение IAM-систем снизило вероятность инцидентов, связанных с неавторизованным доступом, на 70% за последние пять лет.

Для обеспечения устойчивости облачных систем к кибератакам важную роль играет мониторинг и анализ безопасности в реальном времени. Современные облачные провайдеры предлагают инструменты для постоянного мониторинга трафика и событий безопасности. Например, AWS использует систему Amazon GuardDuty для анализа активности в облачных учетных записях, сетевого трафика и логов, что позволяет оперативно выявлять подозрительную активность, такую как несанкционированные попытки доступа или аномалии в использовании ресурсов [2]. В 2022 году Amazon сообщила, что применение GuardDuty позволило более чем в 50% случаев предотвратить серьезные инциденты безопасности еще на

DOI 10.46320/2073-4506-2024-6a-3

этапе их зарождения, что подчеркивает важность таких систем для защиты облачной инфраструктуры.

Одним из инновационных методов защиты является использование искусственного интеллекта и машинного обучения (AI/ML) для выявления и предотвращения угроз. Эти технологии анализируют большие объемы данных, включая сетевой трафик, логи доступа и другие параметры, для обнаружения аномалий и возможных атак. Например, компания Microsoft в своей облачной платформе Azure применяет технологию Azure Sentinel, которая использует AI для автоматического анализа и корреляции данных с целью выявления сложных угроз, таких как продвинутые устойчивые угрозы (APT) или попытки проникновения в систему через уязвимости. По данным компании, использование Azure Sentinel в 2023 году позволило сократить время реакции на киберинциденты на 75%, что значительно повышает скорость устранения угроз и предотвращает их развитие.

Для обеспечения защиты данных на уровне приложений и пользователей также активно применяется технология контейнеризации и виртуализация приложений. Контейнеризация, с помощью таких технологий, как Docker и Kubernetes, позволяет изолировать приложения и их зависимости в контейнерах, что повышает уровень безопасности, ограничивая влияние уязвимостей одного компонента системы на другие. В 2023 году более 60% организаций, использующих облачные платформы, внедрили контейнеризацию как метод защиты данных и управления приложениями, что подтверждает эффективность данного подхода в контексте минимизации рисков.

Еще одним ключевым элементом защиты облачных систем является резервное копирование и восстановление данных (backup and recovery). Облачные провайдеры, такие как AWS и Azure, предлагают встроенные решения для автоматического создания резервных копий данных и их восстановления в случае сбоев или кибератак. Применение технологий резервного копирования позволяет минимизировать потери данных даже в случае DDoS-атак или взлома систем. Важно, что автоматизация процесса резервирования и регулярное тестирование восстановления данных являются неотъемлемыми аспектами защиты в облачных средах.

Роль облачных провайдеров в обеспечении безопасности данных и инфраструктуры является критической, поскольку они предоставляют основу для работы современных облачных информационных систем. Ответственность за безопасность в облачных средах делится между провайдером и пользователем, где провайдеры отвечают за инфраструктуру и базовые сервисы, а клиенты — за данные, доступ и настройку безопасности. Такая модель называется «моделью разделенной ответственности» (shared responsibility model). Она

DOI 10.46320/2073-4506-2024-6a-3

определяет границы ответственности сторон и требует от провайдеров высокого уровня профессионализма и использования современных технологий для защиты инфраструктуры.

Облачные провайдеры, такие как Amazon Web Services (AWS), Microsoft Azure и Google Cloud, играют ключевую роль в обеспечении безопасности физической и виртуальной инфраструктуры. Они обеспечивают защиту на уровне дата-центров, включая контроль физического доступа, видеонаблюдение и системы защиты от природных катастроф. Виртуальная безопасность обеспечивается за счет сегментации сетей, применения продвинутых механизмов шифрования и систем мониторинга, что позволяет изолировать данные одного клиента от данных другого и предотвращать межсегментные утечки.

Основным компонентом обеспечения безопасности на стороне провайдеров является предоставление инструментов и сервисов для защиты данных. Например, AWS предлагает сервисы шифрования данных, такие как AWS Key Management Service (KMS), который позволяет клиентам централизованно управлять шифрованием и защитой ключей, обеспечивая безопасность данных как в процессе хранения, так и при передаче. Google Cloud предлагает аналогичные сервисы через Cloud Key Management. Microsoft Azure обеспечивает возможности шифрования с помощью Azure Key Vault. Эти системы позволяют клиентам создавать, управлять и контролировать доступ к ключам шифрования, что значительно снижает риски утечек данных.

Помимо шифрования, провайдеры предлагают инструменты для мониторинга и управления доступом. Например, AWS использует сервис Amazon GuardDuty, который анализирует данные о сети, события безопасности и логи для обнаружения подозрительной активности в облачной среде клиента. Microsoft Azure использует Azure Security Center для мониторинга безопасности и рекомендаций по усилению защиты. Google Cloud имеет аналогичную систему — Security Command Center. Эти сервисы позволяют пользователям отслеживать инциденты безопасности в реальном времени и быстро реагировать на потенциальные угрозы, используя машинное обучение и автоматические алгоритмы для выявления аномалий.

Облачные провайдеры также играют важную роль в обеспечении безопасности сетевой инфраструктуры. Они предлагают инструменты для защиты сетевых ресурсов, такие как виртуальные частные сети (VPN), фаерволы, системы предотвращения вторжений (IPS) и балансировщики нагрузки, которые помогают защитить облачные ресурсы от внешних атак. Например, AWS предлагает AWS Shield для защиты от DDoS-атак, который использует многоуровневый подход для защиты приложений и сервисов от попыток перегрузить их трафиком. Microsoft Azure предлагает аналогичный сервис Azure DDoS Protection, который

DOI 10.46320/2073-4506-2024-6a-3

автоматически адаптируется к изменениям в трафике и защищает от атаки, обеспечивая устойчивость облачных приложений.

Еще одной важной областью, за которую отвечают провайдеры, является обеспечение соответствия требованиям законодательства и стандартам безопасности. Крупные облачные провайдеры придерживаются строгих стандартов безопасности и проходят сертификацию по таким международным нормам, как ISO/IEC 27001, SOC 1, SOC 2 и SOC 3, а также стандартам безопасности платежных карт PCI DSS. Это гарантирует, что клиенты могут использовать облачные системы для обработки конфиденциальных данных, соответствующих строгим требованиям безопасности. Например, многие провайдеры предлагают специализированные решения для организаций, работающих с данными в здравоохранении (соответствие HIPAA) или финансовом секторе (соответствие GDPR и PCI DSS).

Однако, несмотря на все усилия облачных провайдеров, безопасность остается совместной ответственностью. Важным аспектом является осведомленность клиентов о том, что облачные провайдеры отвечают за безопасность инфраструктуры, а пользователи — за защиту своих данных, управление доступом и настройку сервисов. Примером может служить случай с компанией Capital One, где несмотря на высокий уровень защиты со стороны AWS, утечка данных произошла из-за ошибки в настройке брандмауэра, что подчеркивает необходимость внимательного отношения клиентов к конфигурации безопасности своих облачных ресурсов.

Провайдеры также активно развивают системы автоматического реагирования на инциденты, что позволяет минимизировать человеческий фактор в управлении безопасностью. Например, системы автоматического масштабирования могут реагировать на всплески трафика, вызванные DDoS-атаками, увеличивая вычислительные мощности и предотвращая простои сервисов. Это помогает клиентам поддерживать доступность их приложений даже в условиях повышенной нагрузки. Провайдеры также активно внедряют искусственный интеллект и машинное обучение для автоматического выявления и предотвращения угроз.

Инновационные подходы к защите данных в облачных системах играют решающую роль в противодействии постоянно развивающимся киберугрозам. Современные технологии защиты данных в облаке строятся на использовании искусственного интеллекта (ИИ), машинного обучения, блокчейн-технологий, а также на принципах «нулевого доверия» (Zero Trust) и гомоморфного шифрования. Эти подходы обеспечивают более высокие уровни защиты и позволяют компаниям эффективно минимизировать риски, связанные с утечками данных, кибератаками и нарушением конфиденциальности.

DOI 10.46320/2073-4506-2024-6a-3

Одним из ключевых инновационных подходов является применение искусственного интеллекта и машинного обучения для обеспечения кибербезопасности. Технологии ИИ активно используются для анализа огромных объемов данных, поступающих от облачных систем, и для выявления подозрительных действий, аномалий в поведении пользователей и сетевого трафика. Системы машинного обучения способны обучаться на данных о прошлых атаках и автоматически улучшать алгоритмы обнаружения угроз. Например, такие компании как Microsoft и Google используют ИИ в своих облачных платформах (Microsoft Azure и Google Cloud) для мониторинга активности пользователей и сетевого трафика в реальном времени. В 2022 году Microsoft Azure Sentinel, основанный на ИИ, помог обнаружить и предотвратить более 70% сложных кибератак в корпоративных облаках за счет анализа паттернов поведения и автоматической реакции на угрозы.

Еще одной важной инновацией является внедрение принципа нулевого доверия (Zero Trust) в облачных системах. Zero Trust базируется на предположении, что ни один элемент системы, ни один пользователь или устройство не должны автоматически считаться доверенными. Каждое действие и каждая попытка доступа должны проходить проверку, независимо от того, внутри сети они находятся или снаружи. Это особенно важно в условиях удаленной работы и гибридных облачных инфраструктур, где пользователи и устройства могут подключаться к системе из разных географических мест. Например, Google в рамках своей программы BeyondCorp внедрил Zero Trust архитектуру для внутренней защиты, где каждый запрос доступа к ресурсам проходит строгую проверку, включая многофакторную аутентификацию, анализ контекста устройства и пользователя. Это позволяет значительно снизить риски, связанные с компрометацией учетных данных и сетевых периметров.

Гомоморфное шифрование также становится все более значимым в контексте защиты данных в облаке. Эта технология позволяет выполнять вычисления над зашифрованными данными без необходимости их расшифровки, что решает проблему компрометации данных в процессе обработки. Таким образом, даже в случае утечки или взлома, злоумышленники не смогут получить доступ к содержимому данных. Гомоморфное шифрование активно разрабатывается и используется в таких отраслях, как медицина, финансы и государственные службы, где конфиденциальность данных имеет первостепенное значение. Например, компания IBM развивает технологии гомоморфного шифрования в своей облачной платформе IBM Cloud, предлагая клиентам возможность безопасно обрабатывать конфиденциальные данные, такие как финансовые транзакции или медицинские записи, без риска утечек.

Еще одной значимой инновацией является использование блокчейн-технологий для повышения безопасности данных в облачных системах. Блокчейн предоставляет возможность

DOI 10.46320/2073-4506-2024-6a-3

децентрализованного хранения данных, что делает систему более устойчивой к внешним атакам и нарушению целостности данных. Каждая запись в блокчейне проверяется и зашифрована, что предотвращает возможность несанкционированного изменения данных. Это особенно полезно для критически важных приложений, таких как управление цепочками поставок или финансовые транзакции, где требуется высокая степень доверия и прозрачности. Например, компания IBM использует блокчейн в своих облачных решениях для защиты данных о транзакциях и контроле доступа к системам, что значительно повышает надежность таких приложений и снижает вероятность мошенничества.

Еще одной инновацией является разработка и использование конфиденциальных вычислений (confidential computing). Эта технология основана на создании защищенных сред выполнения программ, которые позволяют обрабатывать данные в защищенных зонах, даже если сама инфраструктура может быть скомпрометирована. Важным элементом этого подхода является использование технологий изоляции на аппаратном уровне, таких как Intel SGX и AMD SEV, которые создают «веренные зоны» внутри процессоров для выполнения критически важных операций. Microsoft Azure активно использует конфиденциальные вычисления для своих клиентов, предлагая защищенные среды выполнения программ для обработки медицинских данных, финансовых транзакций и других конфиденциальных данных. Это позволяет снизить риск утечек, даже если сам облачный провайдер или его инфраструктура подвергнется атаке.

Заключение

Дополнительно стоит отметить растущую роль декларативных моделей безопасности в облачных системах. Такие модели основаны на автоматизированных политиках безопасности, которые применяются к инфраструктуре и приложениям. Например, использование «Infrastructure as Code» (IaC) позволяет компаниям автоматизировать процессы настройки и управления безопасностью облачных систем с помощью кодирования политик безопасности. Это исключает возможность человеческих ошибок и делает процесс настройки более эффективным и безопасным. Такие платформы, как AWS CloudFormation и HashiCorp Terraform, позволяют компаниям внедрять строгие политики безопасности автоматически при развертывании облачных ресурсов, что значительно улучшает соблюдение норм и стандартов безопасности.

Список литературы

1. Николаев А.И., Беляев В.С. Облачные вычисления и безопасность данных: подходы и решения. Вестник МГТУ им. Баумана. Серия: Приборостроение. №4. 2020. С. 12-25.

DOI 10.46320/2073-4506-2024-6a-3

2. Кузнецов В.П., Попов А.В. Информационная безопасность в облачных системах: проблемы и решения. Информационные технологии и вычислительные системы. № 3. 2019. С. 45-58.

3. Смирнов И.Г. Современные методы защиты данных в облачных вычислениях. Научные труды Технического университета. № 5. 2021. С.67-79.

4. Чжао Х., Лю Х. Облачная безопасность: проблемы и решения. Облачные вычисления IEEE, № 7 (2). 2020. С. 64-71.

5. Мелл П., Грэнс Т. Определение облачных вычислений в NIST. Специальное издание Национального института стандартов и технологий. Гейтерсбург, Мэриленд: NIST. 2011.

COMPUTER SECURITY IN CLOUD INFORMATION SYSTEMS: RISKS AND WAYS TO MINIMIZE THEM

Solodovnikov Dmitry Viktorovich
Student of the Far Eastern Federal University
Vladivostok, Russian Federation
Sokolov Alexander Kirillovich
Student of the Far Eastern Federal University
Vladivostok, Russian Federation
Shorokhov Konstantin Dmitrievich
Student of the Far Eastern Federal University
Vladivostok, Russian Federation
Kuchuk Maxim Igorevich
Student of the Far Eastern Federal University
Vladivostok, Russian Federation

Abstract. The article discusses modern innovative approaches to ensuring data security in cloud information systems. The object of the study is national security. The subject of the study is the economics of computer security. The purpose of the study is to reveal the content of computer security in cloud information systems from economic and technical aspects. Technologies such as artificial intelligence, machine learning, homomorphic encryption, blockchain and confidential computing are analyzed, which provide an increased level of data protection and risk minimization. The principle of «Zero Trust» and the use of declarative security models are also discussed as key strategies for ensuring the reliability and sustainability of cloud infrastructures. Examples of their successful application in corporate cloud systems and advantages over traditional data protection methods are described. The innovations under consideration can significantly improve the security of processing and storing confidential information in the context of modern cyber threats.

Key words: cloud information systems, data security, artificial intelligence, machine learning, homomorphic encryption, blockchain, confidential computing, zero trust, data protection, cybersecurity.

References

1. Nikolaev A.I., Belyaev V.S. Cloud computing and data security: approaches and solutions. Bulletin of the Bauman Moscow State Technical University. Series: Instrument engineering. № 4. 2020. P. 12-25.

DOI 10.46320/2073-4506-2024-6a-3

2. Kuznetsov V.P., Popov A.V. Information security in cloud systems: problems and solutions. Information technologies and computing systems. № 3. 2019. P. 45-58.
3. Smirnov I.G. Modern methods of data protection in cloud computing. Scientific papers of the Technical University. № 5. 2021. P.67-79.
4. Zhao H., Liu H. Cloud security: problems and solutions. IEEE Cloud Computing, № 7 (2). 2020. P. 64-71.

DOI 10.46320/2073-4506-2024-6a-3