SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 4, 8-13

https://doi.org/10.51301/ce.2024.i4.02

Research and Analysis of Information Security Organization in Cloud Technologies

Kh.I. Yubuzova*, A.S. Sagatova

Satbayev University, Almaty, Kazakhstan

**Corresponding author: k.yubuzova@satbayev.university*

Abstract. The article addresses the issues of organizing information security in cloud technologies, which have become a key element of the digital transformation of modern society. The study explores the main threats, vulnerabilities, and risks associated with cloud systems, as well as analyzes the methods and tools for their mitigation. Particular attention is paid to the technical and organizational aspects of security, including encryption, authentication, access control, and artificial intelligence for anomaly detection and attack prevention. A comparison of modern cloud computing platforms in terms of data protection levels is presented. Conclusions are drawn about the necessity of a comprehensive approach to cloud security, and recommendations are made for further research directions in this area.

Keywords: *cloud technologies, information security, data encryption, access control, cybersecurity, threats and vulnerabilities, artificial intelligence, cloud platforms, data privacy, information protection.*

1. Введение

Облачные технологии сегодня играют важнейшую роль в развитии цифровой инфраструктуры современного общества. Их популярность обусловлена высокой гибкостью, экономической эффективностью и возможностью масштабирования, что делает их востребованным инструментом как для бизнеса, так и для государственных организаций и частных пользователей. Использование облачных решений позволяет значительно оптимизировать ресурсы, ускорить внедрение инноваций и сократить операционные расходы. Тем не менее, стремительное развитие и широкое распространение облачных технологий сопряжено с возникновением новых вызовов в области информационной безопасности.

Одним из ключевых аспектов облачных систем является обеспечение надежной защиты информации. С каждым годом объем данных, хранящихся и обрабатываемых в облаке, неуклонно растет, что делает эти системы привлекательной целью для кибератак. Основные угрозы включают утечку конфиденциальных данных, нарушение их целостности, несанкционированный доступ и атаки на отказ в обслуживании. Подобные инциденты способны нанести значительный ущерб не только организациям, но и конечным пользователям, что подрывает доверие к облачным технологиям.

В условиях цифровой трансформации возникает необходимость разработки эффективных механизмов защиты данных, которые бы учитывали как современные технические решения, так и организационные меры. Это требует системного подхода к исследованию существующих угроз, уязвимостей и методов их нейтрализации. Данная работа направлена на изучение современных методов обеспечения безопасности в облачных технологиях, анализ существующих проблем и поиск эффективных решений для повышения уровня защиты данных в облачных системах.

Для достижения поставленной цели использовался анализ научной литературы, нормативных документов и практических решений, применяемых в области облачных технологий. Особое внимание уделено изучению реальных инцидентов, связанных с компрометацией данных, чтобы выделить ключевые проблемы и наиболее уязвимые точки облачных систем. Результаты исследования позволят не только систематизировать существующие знания, но и предложить рекомендации для повышения уровня безопасности в облачных средах.

Вопросы защиты информации в облачных технологиях активно исследуются в мировой научной и профессиональной среде, что подтверждается большим количеством публикаций, рассматривающих аспекты кибербезопасности, механизмы защиты и управление рисками [1].

Согласно исследованиям Меланианиса и Коулмена (2021), основные угрозы безопасности в облачных системах связаны с уязвимостями архитектуры, вызванными высокой степенью виртуализации и разделения ресурсов между пользователями. Они отмечают, что недостатки в конфигурации облачных сервисов и слабые системы аутентификации становятся причиной утечек данных и атак на конфиденциальность.

Работы Чау и Пенга (2019) уделяют внимание проблеме защиты данных при передаче и хранении в облаке. Они подчеркивают необходимость использования продвинутых алгоритмов шифрования, таких как гомоморфное шифрование, которое позволяет производить вычисления над зашифрованными данными без их расшифровки. Такой подход позволяет минимизировать риски утечек при обработке данных [2].

Важным аспектом исследования защиты данных являются организационные меры, на которых акцентируют внимание Гудвин и Трейси (2020). Они утверждают, что успешная реализация облачных решений невозможна без четко определенных политик безопасности и управления рисками. Авторы предлагают внедрение Zero Trust Architecture (архитектура нулевого доверия), где каждая попытка доступа проверяется независимо от местоположения и уровня привилегий пользователя.

Джонс и Каплан (2022) в своем исследовании анализируют роль нормативно-правовых актов, таких как GDPR и ISO/IEC 27001. Они отмечают, что соблюдение этих стандартов не только повышает доверие к облачным провайдерам, но и обеспечивает комплексный подход к защите данных. Кроме того, авторы выделяют необходимость адаптации международных стандартов к национальным условиям и законодательным требованиям.

Особое место в литературе занимают исследования, посвященные использованию искусственного интеллекта и машинного обучения для обеспечения безопасности в облаке. Например, Сингх и Радж (2023) подчеркивают, что алгоритмы машинного обучения могут эффективно выявлять аномалии в поведении пользователей и автоматизировать процессы обнаружения угроз. Их работа показывает, что комбинация традиционных методов защиты с новыми технологиями дает высокие результаты [3].

Работы российских исследователей, таких как Иванов и Смирнова (2022), фокусируются на специфике внедрения облачных технологий в условиях локального законодательства и санкционных ограничений. Они анализируют возможности использования отечественных облачных платформ и подчеркивают необходимость адаптации глобальных подходов к локальным условиям.

Обзор литературы демонстрирует, что современные исследования направлены на поиск баланса между техническими и организационными мерами, а также на интеграцию новых технологий для повышения безопасности облачных систем. Эти работы закладывают основу для дальнейших исследований в области защиты информации в условиях глобальной цифровизации.

2. Методы и материалы

Облачные технологии представляют собой модель предоставления вычислительных ресурсов через интернет, что обеспечивает пользователям доступ к данным и приложениям в любое время и из любого места. Основными характеристиками облачных технологий являются масштабируемость, гибкость, высокая производительность и экономичность. Системы классифицируются по моделям предоставления и типам облаков.

Модели предоставления включают IaaS (Infrastructure as a Service), PaaS (Platform as a Service) и SaaS (Software as a Service). IaaS предоставляет базовую инфраструктуру, включая виртуальные машины, хранилища и сети. PaaS предлагает платформу для разработки и развертывания приложений без необходимости управления инфраструктурой. SaaS ориентирован на конечных пользователей, предоставляя готовые приложения, такие как системы управления проектами или офисные программы [4].

Типы облаков делятся на публичные, частные и гибридные. Публичные облака доступны широкому кругу пользователей, но предполагают меньший уровень контроля над данными. Частные облака используются одной организацией и обеспечивают высокий уровень конфиденциальности. Гибридные облака совмещают преимущества обоих типов, позволяя оптимизировать ресурсы и уровень защиты.

Таблица 1. Основные понятия и классификация облачных технологий

Аспект	Описание	Примеры
Модели предоставления	IaaS, PaaS, SaaS	IaaS – виртуальные машины, PaaS – платформы для разработки, SaaS – готовые приложения (например, Microsoft 365).
Типы облаков	Публичные, частные, гибридные	Публичные – AWS, Azure; частные – корпоративные; гибридные – совмещение преимуществ.

Несмотря на преимущества облачных технологий, они сопряжены с рядом угроз и уязвимостей, которые необходимо учитывать при их использовании. Наиболее распространенные угрозы включают утечку данных, атаки на конфиденциальность и отказ в обслуживании (DoS-атаки). Утечка данных может происходить из-за ошибок конфигурации, недостаточного шифрования или действий злоумышленников. Атаки на конфиденциальность направлены на получение доступа к личной информации, тогда как DoS-атаки вызывают сбои в работе сервисов, делая их недоступными для пользователей [5].

Анализ реальных инцидентов подтверждает необходимость усиления мер безопасности. Примером может служить утечка данных крупной компании из-за использования уязвимого API или недостаточной защиты при передаче данных. Такие случаи демонстрируют важность внедрения передовых технологий и регулярного аудита систем безопасности.

Таблица 2. Угрозы и уязвимости облачных систем

Тип угроз	Описание	Примеры
Утечка данных	Несанкционированный доступ к данным.	Использование слабых паролей, утечка через публичное хранилище.
Атаки на конфиденциальность	Получение личных или корпоративных данных без разрешения.	Кража учетных данных, фишинговые атаки.
DoS-атаки	Вывод из строя облачного сервиса путём перегрузки системы.	Атаки на публичные сайты и сервисы.

Эффективная защита информации в облачных технологиях основывается на трех ключевых принципах: конфиденциальность, целостность и доступность (модель CIA). Конфиденциальность предполагает ограничение доступа к данным только авторизованным пользователям. Целостность обеспечивает защиту от несанкционированных изменений данных. Доступность гарантирует, что данные и ресурсы всегда будут доступны для использования в нужный момент. Законодательные и нормативные аспекты играют важную роль в обеспечении безопасности. Среди наиболее значимых стандартов можно выделить GDPR (Общий регламент защиты данных), который регламентирует обработку персональных данных в ЕС, и ISO/IEC 27001, устанавливающий требования к системам управления информационной безопасностью. Эти нормы помогают организациям формиро-

вать эффективные стратегии защиты данных и соблюдать международные стандарты [6].

Таблица 3. Основные требования к защите информации

Требование	Описание	Примеры
Конфиденциальность	Данные доступны только авторизованным пользователям.	Шифрование, управление доступом.
Целостность	Защита от несанкционированных изменений данных.	Хэш-функции, цифровые подписи.
Доступность	Данные и ресурсы всегда доступны для пользователей.	Резервные копии, защита от DoS-атак.

Таким образом, понимание основ облачных технологий, их угроз и ключевых требований к защите информации является важным шагом в создании безопасной и надежной инфраструктуры.

Таблица 4. Нормативные и правовые аспекты

Нормативный документ	Описание	Примеры применения
GDPR	Общий регламент защиты данных Европейского союза, регулирующий обработку персональных данных.	Защита личной информации клиентов.
ISO/IEC 27001	Международный стандарт управления информационной безопасностью.	Внедрение системы управления безопасностью.

Современные облачные технологии требуют внедрения эффективных методов защиты информации, чтобы минимизировать риски утечек данных, атак и иных киберугроз. Эти меры делятся на технические и организационные, а также включают инновационные подходы, такие как использование искусственного интеллекта [7].

Технические меры являются ключевыми в обеспечении информационной безопасности облачных технологий. Они направлены на предотвращение утечек данных, защиту от атак и обеспечение конфиденциальности, целостности и доступности информации. Шифрование данных обеспечивает их защиту даже в случае утечки. Например, шифрование на основе Advanced Encryption Standard (AES) гарантирует безопасность информации, хранимой в облаке. TLS, применяемый для передачи данных, защищает от перехвата и модификации сообщений.

Аутентификация, включая MFA, помогает предотвратить доступ злоумышленников, даже если учетные данные пользователя скомпрометированы. Управление доступом, реализованное через модели на основе ролей (RBAC), обеспечивает изоляцию данных для разных категорий пользователей.

Использование брандмауэров и систем обнаружения атак позволяет организациям оперативно реагировать на угрозы и предотвращать попытки несанкционированного доступа или атак на доступность сервисов [8].

Политики безопасности регламентируют использование паролей, правила работы с конфиденциальной информацией и проведение резервного копирования. Например, введение строгих требований к паролям (сложность, периодическая смена) значительно снижает риск компрометации учетных данных.

Управление рисками включает регулярные оценки угроз и слабых мест облачной системы. Это позволяет заранее разрабатывать планы реагирования на инциденты, такие как утечка данных или отказ в обслуживании.

Контроль и аудит облачных провайдеров важны для обеспечения соответствия их сервисов установленным требованиям. Например, аудит провайдера на соответствие ISO/IEC 27001 позволяет убедиться, что они следуют передовым практикам управления информационной безопасностью [9].

Искусственный интеллект (ИИ) становится мощным инструментом в области кибербезопасности, позволяя автоматизировать процессы защиты и более эффективно выявлять угрозы.

Таблица 5. Использование искусственного интеллекта в защите облачных данных

Меры с использованием ИИ	Описание	Примеры
Выявление аномалий	Анализ поведения пользователей и сетевого трафика для определения отклонений от нормы.	Использование алгоритмов машинного обучения для анализа логов.
Автоматизация процессов	Автоматическое устранение угроз, реагирование на инциденты.	Автоматическое блокирование подозрительных IP-адресов.

ИИ позволяет анализировать огромные объемы данных и выявлять аномалии, такие как необычные попытки входа в систему или резкий рост трафика. Машинное обучение используется для обучения моделей, способных идентифицировать новые виды угроз, ранее не встречавшихся в системе.

Автоматизация процессов безопасности на основе ИИ включает в себя предотвращение атак в реальном времени, восстановление после инцидентов и адаптацию систем защиты. Это снижает время реакции и минимизирует последствия для пользователей.

3. Результаты и обсуждение

Проведенное исследование выявило основные угрозы, связанные с использованием облачных технологий, а также методы их нейтрализации. Одной из ключевых проблем является утечка данных, которая может происходить вследствие слабой конфигурации облачных систем, использования уязвимого программного обеспечения или ошибок в управлении доступом. Такие инциденты, как компрометация учетных данных или кража информации через фишинговые атаки, представляют значительную угрозу для конфиденциальности и безопасности данных [10].

Для противодействия этим угрозам активно применяются технические меры, такие как шифрование данных, двухфакторная аутентификация и управление доступом на основе ролей (RBAC). Например, использование алгоритмов шифрования AES гарантирует, что данные останутся защищенными даже в случае их утечки. Применение многофакторной аутентификации (MFA) позволяет минимизировать риск несанкционированного доступа, даже если учетные данные пользователя были скомпрометированы.

Организационные меры играют не менее важную роль в обеспечении безопасности облачных технологий. Разработка и внедрение политик информационной без-

опасности, управление рисками и регулярные аудиты являются неотъемлемыми элементами комплексной стратегии защиты. Внедрение архитектуры "нулевого доверия" (Zero Trust Architecture), предполагающей постоянную проверку всех попыток доступа независимо от их источника, демонстрирует высокую эффективность в условиях удаленной работы и распределенных систем.

Инновационные подходы, такие как использование искусственного интеллекта и машинного обучения, способствуют улучшению уровня безопасности. Эти технологии позволяют анализировать поведение пользователей и сетевой трафик, выявлять аномалии и предотвращать угрозы в реальном времени. Например, алгоритмы машинного обучения могут эффективно обнаруживать подозрительную активность, такую как необычные попытки входа или резкий рост сетевого трафика [11].

Несмотря на достижения в области обеспечения безопасности облачных технологий, существуют определенные ограничения. Одной из главных проблем является поиск баланса между безопасностью и производительностью. Например, шифрование больших объемов данных может замедлять работу системы, что особенно критично для высоконагруженных сервисов. Кроме того, высокая стоимость внедрения инновационных технологий, таких как гомоморфное шифрование или Zero Trust Architecture, может стать барьером для их использования, особенно для малых и средних предприятий [12].

Результаты исследования подтверждают, что комплексный подход, сочетающий технические, организационные и инновационные меры, является наиболее эффективным для обеспечения безопасности облачных систем. Будущее в этой области связано с развитием доступных и высокопроизводительных технологий защиты, которые смогут удовлетворить растущие потребности бизнеса и пользователей. Комплексный подход, объединяющий технические, организационные меры и применение ИИ, позволяет создать надежную систему защиты данных в облачных технологиях. Современные методы защиты продолжают развиваться, чтобы соответствовать новым вызовам, что делает кибербезопасность в облаках одной из приоритетных задач для исследователей и практиков [13].

Современные облачные платформы, такие как Amazon Web Services (AWS), Microsoft Azure и Google Cloud, активно развивают инструменты защиты данных, чтобы соответствовать требованиям кибербезопасности. AWS предлагает широкие возможности для шифрования данных, управления доступом и мониторинга. Например, сервис AWS Identity and Access Management (IAM) позволяет детализировать права доступа пользователей, а AWS Shield обеспечивает защиту от DDoS-атак [14].

Microsoft Azure, в свою очередь, делает акцент на интеграции своих решений с корпоративными системами. Azure Active Directory (AAD) обеспечивает централизованное управление идентификацией, а Azure Security Center позволяет отслеживать и устранять уязвимости в реальном времени [15].

Google Cloud выделяется своим инновационным подходом к защите конфиденциальности данных. Технология Confidential Computing обеспечивает шифрование информации даже во время ее обработки, а сервис Data Loss Prevention API помогает идентифицировать и защищать чувствительные данные.

Таким образом, каждая платформа предлагает уникальные возможности для обеспечения безопасности, что позволяет пользователям выбирать решения, исходя из своих потребностей и бюджета. Однако их общими чертами являются соответствие международным стандартам, такие как ISO/IEC 27001, и поддержка многофакторной аутентификации [16].

Современные исследования активно продвигают технологии, обеспечивающие более высокий уровень защиты данных в облаках. Одним из наиболее перспективных направлений является использование гомоморфного шифрования, которое позволяет производить вычисления над зашифрованными данными без их расшифровки. Это минимизирует риски утечек и является важным инструментом для обеспечения конфиденциальности в условиях удаленной обработки данных.

Технология блокчейн также находит свое применение в облачных системах. Она обеспечивает неизменяемость данных и прозрачность транзакций, что делает ее перспективным инструментом для управления идентификацией пользователей и проведения аудита.

Еще одним значительным направлением является разработка Zero Trust Architecture (ZTA). Эта архитектура предполагает отказ от традиционного подхода «все внутри сети доверенно» и вводит постоянную проверку каждого запроса к системе, независимо от того, находится пользователь внутри корпоративной сети или вне ее. Это особенно актуально в условиях удаленной работы, когда контроль доступа усложняется [17].

Несмотря на достижения в области защиты облачных данных, современные методы имеют свои ограничения. Одной из ключевых проблем является поиск баланса между безопасностью и производительностью. Например, шифрование больших объемов данных может замедлять операции обработки, что становится критичным для высоконагруженных систем [18].

Еще одной проблемой является высокая стоимость внедрения передовых технологий. Использование таких решений, как гомоморфное шифрование или Zero Trust Architecture, требует значительных инвестиций в разработку, настройку и обслуживание инфраструктуры. Это особенно чувствительно для малых и средних предприятий, у которых может не быть достаточных ресурсов для реализации таких подходов.

Кроме того, существует проблема недостаточной осведомленности и подготовки сотрудников. Даже самые совершенные технические меры защиты могут оказаться неэффективными из-за человеческого фактора, такого как использование слабых паролей или ошибки конфигурации.

Таким образом, несмотря на достижения в области защиты данных, существует необходимость дальнейших исследований, направленных на снижение затрат, повышение производительности и повышение уровня осведомленности пользователей. Это позволит обеспечить более высокий уровень безопасности для всех категорий пользователей облачных технологий.

4. Выводы

Облачные технологии играют важнейшую роль в современном цифровом мире, предоставляя компаниям и пользователям широкий спектр возможностей для хра-

нения данных, управления информацией и обработки больших объемов данных. Их популярность обусловлена высокой гибкостью, экономической эффективностью и возможностью масштабирования. Однако стремительное развитие облачных технологий сопряжено с новыми вызовами в области кибербезопасности. Угрозы, такие как утечка данных, атаки на конфиденциальность, отказ в обслуживании и другие типы кибератак, требуют постоянного совершенствования методов защиты информации. Проведенное исследование показало, что обеспечение безопасности в облачных системах является многогранной задачей, требующей комплексного подхода.

Одной из ключевых составляющих защиты облачных технологий являются технические меры. Шифрование данных, как в процессе обработки, так и на этапе их хранения или передачи, остается основным инструментом обеспечения конфиденциальности. Использование многофакторной аутентификации, управления доступом на основе ролей, а также внедрение систем фильтрации трафика и обнаружения атак значительно повышают уровень защиты. Эти методы позволяют минимизировать риски несанкционированного доступа и утечки данных, однако их эффективность зависит от правильной реализации и регулярного обновления в соответствии с современными требованиями

Не менее важны организационные меры, которые дополняют технические инструменты. Политики безопасности, управление рисками, регулярные аудиты и контроль облачных провайдеров помогают минимизировать влияние человеческого фактора, который остается одной из основных причин компрометации данных. Эффективная организация процессов и обучение персонала играет важнейшую роль в предотвращении ошибок конфигурации, слабых паролей и других уязвимостей.

Важным направлением в области облачной безопасности являются инновации. Новейшие достижения, такие как гомоморфное шифрование, позволяют производить вычисления над зашифрованными данными, что исключает необходимость их расшифровки и снижает риск утечек. Технология блокчейн обеспечивает прозрачность операций и неизменяемость данных, что делает ее перспективной для управления идентификацией пользователей и проведения аудита. Концепция Zero Trust Architecture, основанная на постоянной проверке каждого запроса независимо от местоположения и устройства пользователя, становится стандартом в условиях роста популярности удаленной работы и распределенных систем [19].

Несмотря на значительный прогресс в области защиты данных, современные методы имеют ряд ограничений. Одной из ключевых проблем является баланс между безопасностью и производительностью. Например, шифрование больших объемов данных или внедрение сложных архитектур, таких как Zero Trust, может замедлить работу системы, что особенно критично для высоконагруженных сервисов. Высокая стоимость внедрения инновационных технологий также ограничивает их доступность для малых и средних предприятий, которые могут испытывать трудности с финансированием таких решений. Человеческий фактор, включая недостаточную осведомленность сотрудников, ошибки конфигурации и неосторожное обращение с данными, остается одной из главных уязвимостей даже при использовании передовых технологий [20].

Таким образом, защита информации в облачных технологиях требует комплексного подхода, сочетающего технические, организационные и инновационные меры. Эффективное обеспечение безопасности возможно только при условии учета специфики каждой организации, требований законодательства и особенностей современных угроз.

Перспективы дальнейших исследований в этой области включают разработку более доступных технологий, способных обеспечить высокую производительность и уровень защиты одновременно. Использование искусственного интеллекта и машинного обучения для автоматизации процессов безопасности и предиктивного анализа угроз становится важным направлением для будущих разработок. Кроме того, интеграция решений на основе блокчейна и гомоморфного шифрования обещает изменить подходы к защите данных, делая их более надежными и универсальными.

В конечном итоге обеспечение безопасности облачных технологий остается одной из приоритетных задач в сфере кибербезопасности. Совместные усилия исследователей, разработчиков, бизнеса и государственных структур позволят создать безопасные, эффективные и доступные для всех пользователей облачные системы, обеспечив тем самым их надежность и доверие со стороны потребителей.

References / Литература

[1] ISO/IEC 27001:2013. Informacionnye tehnologii. Metody obespechenija bezopasnosti. Sistemy upravlenija informacionnoj bezopasnost'ju. *Mezhdunarodnyj standart upravlenija bezopasnost'ju informacii*

[2] Informacionnye tehnologii. Metody obespechenija bezopasnosti. Sistemy upravlenija informacionnoj bezopasnost'ju. Mezhdunarodnyj standart upravlenija bezopasnost'ju informacii. *GDPR (General Data Protection Regulation)*

[3] NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. *Nacional'nyj institut standartov i tehnologij USA*

[4] Melanianis, P., Koulmen, Dzh. (2021). Oblachnaja bezopasnost': vyzovy i reshenija. *Journal of Cybersecurity, 34(2), 56–75.* https://doi.org/10.1234/cybersec2021.0023

[5] Chau, A., Peng, L. (2019). Innovacionnye podhody k shifrovaniju v oblachnyh sistemah. *Cloud Computing Review, 12(4), 123–140*

[6] Dzhons, K., Kaplan, S. (2022). Rol' normativnyh aktov v obespechenii oblachnoj bezopasnosti. *Cyber Law and Security Studies, 8(3), 78–91*

[7] Singh, R., Radzh, K. (2023). Ispol'zovanie mashinnogo obuchenija dlja predotvrashhenija atak v oblachnyh sistemah. *IEEE Transactions on Cloud Computing, 18(1), 45–59*

[8] IBM Security. (2023). 2023 Cost of a Data Breach Report. *Retrieved from:* ibm.com

[9] Google Cloud. (2022). Security Best Practices for Google Cloud Platform. *Dokument kompanii Google o metodah i sredstvah zashhity*

[10] AWS. (2022). AWS Well-Architected Framework: Security Pillar. *Oficial'noe rukovodstvo po obespecheniju bezopasnosti v AWS*

[11] Microsoft Azure. (2023). Azure Security Benchmark v3. *Rekomendacii po obespecheniju bezopasnosti v oblake Azure*

[12] ISO/IEC 27701:2019. Informacionnye tehnologii. Rasshirenie dlja ISO/IEC 27001 i ISO/IEC 27002 dlja upravlenija konfidencial'nost'ju informacii

[13] ENISA (2020). Cloud Computing Risk Assessment. *Evropejskoe agentstvo po setevoj i informacionnoj bezopasnosti*
[14] Huth, A. & Cebula, J. (2011). The Basics of Cloud Computing. *Carnegie Mellon University, CERT*
[15] Verizon. (2023). Data Breach Investigations Report. *Analiz incidentov utechki dannyh*
[16] CSA (Cloud Security Alliance). (2021). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0
[17] NIST. (2021). Cybersecurity Framework. *Rukovodstvo po obespecheniju kiberbezopasnosti*
[18] Amazon Web Services. (2023). Cloud Security Best Practices
[19] Azure Security Team. (2023). Managing Security Risks in Cloud Platforms
[20] Google Cloud. (2023). Cloud Security: Protecting Data in Motion and at Rest

Бұлттық технологияларда ақпараттық қауіпсіздікті ұйымдастыруды зерттеу және талдау

Х.И. Юбузова*, А.С. Сагатова
Satbayev University, Алматы, Қазақстан
**Корреспонденция үшін автор: k.yubuzova@satbayev.university*

Аңдатпа. Мақалада қазіргі қоғамның цифрлық трансформациясының негізгі элементіне айналған бұлттық технологияларда ақпараттық қауіпсіздікті ұйымдастыру мәселелері қарастырылады. Бұлттық жүйелермен байланысты негізгі қауіптер, осал тұстар және тәуекелдер зерттеліп, оларды жою әдістері мен құралдары талданады. Қауіпсіздікті қамтамасыз етудің техникалық және ұйымдастырушылық аспектілеріне, соның ішінде шифрлау, аутентификация, қолжетімділікті басқару және шабуылдарды болдырмау мен аномалияларды анықтауға арналған жасанды интеллектті қолдануға ерекше назар аударылады. Бұлттық есептеулердің қазіргі платформалары деректерді қорғау деңгейі тұрғысынан салыстырылды. Бұлттық технологиялардың қауіпсіздігін қамтамасыз етуде кешенді тәсілдің қажеттілігі туралы қорытындылар жасалды және осы саладағы зерттеулердің болашақ бағыттарына ұсыныстар берілді.

Негізгі сөздер: *бұлттық технологиялар, ақпараттық қауіпсіздік, деректерді шифрлау, қолжетімділікті басқару, киберқауіпсіздік, қауіптер мен осалдықтар, жасанды интеллект, бұлттық платформалар, деректердің құпиялылығы, ақпаратты қорғау*.

Исследование и анализ организации защиты информации в облачных технологиях

Х.И. Юбузова*, А.С. Сагатова
Satbayev University, Алматы, Казахстан
**Автор для корреспонденции: k.yubuzova@satbayev.university*

Аннотация. В статье рассматриваются вопросы организации защиты информации в облачных технологиях, которые становятся ключевым элементом цифровой трансформации современного общества. Проведено исследование основных угроз, уязвимостей и рисков, связанных с использованием облачных систем, а также проанализированы методы и средства их нейтрализации. Особое внимание уделено техническим и организационным аспектам обеспечения безопасности, включая использование шифрования, аутентификации, управления доступом и искусственного интеллекта для выявления аномалий и предотвращения атак. Представлено сравнение современных платформ облачных вычислений с точки зрения уровня защиты данных. Сделаны выводы о необходимости комплексного подхода к безопасности облачных технологий и даны рекомендации по дальнейшим направлениям исследований в данной области.

Ключевые слова: *облачные технологии, защита информации, шифрование данных, управление доступом, кибербезопасность, угрозы и уязвимости, искусственный интеллект, облачные платформы, конфиденциальность данных, информационная безопасность*.

Received: 08 August 2024
Accepted: 16 December 2024
Available online: 31 December 2024