

данных». СПб.: Питер, 2019.

4. Шаповалов, В.В. «Криптография: теория и практика». М.: Альпина Паблишер, 2022.

5. Кузнецов, А.Ю. «Информационная безопасность в цифровом обществе». М.: ИНФРА-М, 2021.

УДК 004.451.42

П.С. Мырадов, А.М. Хамраев

Государственный энергетический институт
Мары, Туркменистан

БЕЗОПАСНОСТЬ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

***Аннотация.** Облачные вычисления стали важной частью современной цифровой инфраструктуры, предоставляя пользователям гибкость, масштабируемость и экономию ресурсов. Однако с распространением облачных технологий возросли риски безопасности данных, связанные с утечками, несанкционированным доступом и другими киберугрозами. В данной статье рассматриваются ключевые аспекты безопасности данных в облачных вычислениях, включая используемые механизмы защиты, регуляторные требования и современные подходы к управлению рисками. Особое внимание уделено применению криптографических методов, аутентификации и современных технологий для повышения защищённости данных.*

P.S. Myradov, A.M. Hamrayev

The State Energy Institute
Mary, Turkmenistan

DATA SECURITY IN CLOUD COMPUTING

***Abstract.** Cloud computing has become a vital part of modern digital infrastructure, offering users flexibility, scalability, and resource efficiency. However, the spread of cloud technologies has increased data security risks, including leaks, unauthorized access, and other cyber threats. This article explores key aspects of data security in cloud computing, focusing on protection mechanisms, regulatory requirements, and modern risk management approaches. Special attention is given to the use of cryptographic methods, authentication, and advanced technologies to enhance data protection.*

Введение

Облачные вычисления кардинально изменили подход к хранению и обработке данных, обеспечив доступ к ресурсам в режиме реального времени и снизив затраты на ИТ-инфраструктуру. Вместе с

тем, использование облачных сервисов привело к возникновению новых вызовов в области безопасности данных, поскольку данные покидают корпоративные границы и хранятся на сторонних платформах.

Основные цели данной статьи – изучить ключевые угрозы безопасности данных в облачных вычислениях, описать применяемые методы защиты и предложить перспективные подходы к обеспечению безопасности в будущем.

Обзор облачных вычислений и их архитектуры

Виды облаков:

Публичные облака (например, AWS, Azure) предоставляют услуги широкому кругу пользователей.

Частные облака создаются для одной организации с полным контролем над данными.

Гибридные облака объединяют преимущества частных и публичных моделей.

Сервисные модели:

IaaS (Infrastructure as a Service) предоставляет доступ к виртуализированной инфраструктуре.

PaaS (Platform as a Service) предлагает платформу для разработки и развертывания приложений.

SaaS (Software as a Service) предоставляет готовые приложения пользователям по подписке.

Проблемы безопасности в облачных вычислениях

Использование облачных технологий связано с рядом угроз:

Утечка данных: Данные могут быть скомпрометированы из-за ошибок конфигурации или атак.

DDoS-атаки: Злоумышленники могут перегружать облачные сервисы, нарушая их работу.

Неавторизованный доступ: При недостаточной аутентификации злоумышленники получают доступ к критическим данным.

Кроме того, распределённая природа облаков затрудняет контроль доступа и управление данными, что повышает риски конфиденциальности.

Методы и механизмы обеспечения безопасности данных

Криптография:

Использование симметричного и асимметричного шифрования для защиты данных при хранении и передаче. Например, AES и RSA –

популярные алгоритмы шифрования.

Аутентификация и управление доступом:

Включает применение многофакторной аутентификации (MFA) и токенов доступа.

Защита данных в состоянии покоя и при передаче:

Используются технологии, такие как TLS и VPN, для защиты передаваемых данных.

Блокчейн:

Обеспечивает неизменяемость данных и контроль их целостности благодаря децентрализованной архитектуре.

Регуляторные требования и стандарты

ISO/IEC 27001 – стандарт управления информационной безопасностью.

GDPR – Общий регламент по защите данных в ЕС.

PCI DSS – стандарт для защиты данных держателей карт в финансовом секторе.

Провайдеры облачных услуг должны соответствовать этим требованиям и обеспечивать прозрачность в управлении данными.

Современные технологии и тенденции в области безопасности

Искусственный интеллект (ИИ) и машинное обучение (МО):

ИИ используется для выявления аномалий в поведении пользователей и обнаружения угроз.

Модель Zero Trust:

Подход, при котором всем пользователям и устройствам проверяется доступ, независимо от их местоположения.

Гомоморфное шифрование:

Обеспечивает возможность обработки зашифрованных данных без их расшифровки. Это перспективное направление для облачных вычислений.

Кейс-стади: Реальные примеры атак и меры по защите

Примером успешной атаки является утечка данных компании Capital One в 2019 году, когда конфиденциальная информация была скомпрометирована из-за уязвимости конфигурации. В качестве меры защиты компании внедряют автоматизированные системы контроля конфигураций и применяют шифрование данных.

Обсуждение и перспективы развития

Основные вызовы безопасности в облачных вычислениях включают сложность управления доступом и необходимость в

постоянной адаптации к новым угрозам. Будущие исследования могут быть направлены на улучшение механизмов аутентификации и разработку новых методов шифрования.

Заключение

Обеспечение безопасности данных в облачных вычислениях требует комплексного подхода, включающего использование криптографии, аутентификации и соответствие нормативным требованиям. Внедрение современных технологий, таких как ИИ и гомоморфное шифрование, открывает новые возможности для повышения безопасности.

Список использованных источников

1. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology.
2. ISO/IEC 27001:2013. Information security management systems – Requirements.
3. European Parliament. (2016). General Data Protection Regulation (GDPR).
4. Stallings, W. (2019). Cryptography and Network Security: Principles and Practice. Pearson.
5. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds.

УДК 316.77

M. D. Nikitina, G. V. Pribylskaya
Belarusian National Technical University
Minsk, Belarus

THE IMPACT OF INFORMATION TECHNOLOGY ON OUR LIVES: FROM ROBOTS TO DIGITAL MARKETING

***Abstract.** The article deals with the introduction of new technologies in the modern world. The digital transformation of society is large-scale changes caused by the introduction of digital technologies into all spheres of human life: science, medicine, sports, culture. Technologies are becoming more advanced every year; in the future we will see how actively artificial intelligence will be introduced into human everyday life.*

М. Д. Никитина, Г. В. Прибыльская