Сычев Д.И. Основы безопасности облачных данных: преодоление проблем и внедрение передового опыта для надежной защиты // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 20–25

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

# ОСНОВЫ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ДАННЫХ: ПРЕОДОЛЕНИЕ ПРОБЛЕМ И ВНЕДРЕНИЕ ПЕРЕДОВОГО ОПЫТА ДЛЯ НАДЕЖНОЙ ЗАЩИТЫ

**Сычев Д.И.**
*ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: s.denis_2001@mail.ru*

**На текущем уровне развития информационных технологий, организации все больше полагаются на облачные вычисления для хранения своих данных и потребностей приложений.. Сосредоточив внимание на современных угрозах и стратегиях защиты конфиденциальной информации, ниже обсуждаются проблемы защиты облачных данных, представлен набор передовых методов снижения этих рисков и выделяются потенциальные области для дальнейших исследований. Предоставленная информация призвана помочь организациям разработать комплексные стратегии облачной безопасности, обеспечивающие защиту ценных данных в постоянно развивающемся цифровом ландшафте.**

Ключевые слова: Безопасность облачных данных, информационная безопасность, шифрование.

# BASICS OF CLOUD DATA SECURITY: OVERCOMING PROBLEMS AND IMPLEMENTING BEST PRACTICES FOR RELIABLE PROTECTION

**Sychev D.I.**
*St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, Bolshevikov Ave., 22, room 1), e-mail: s.denis_2001@mail.ru*

**At the current level of information technology development, organizations are increasingly relying on cloud computing to store their data and application needs.. Focusing on modern threats and strategies for protecting confidential information, the problems of protecting cloud data are discussed below, a set of best practices for reducing these risks is presented, and potential areas for further research are highlighted. The information provided is intended to help organizations develop comprehensive cloud security strategies that protect valuable data in an ever-evolving digital landscape.**

Keywords: Cloud data security, information security, encryption.

## Введение

В отличие от ранних кибератак, когда злоумышленник атаковал определенный набор IP-адресов или конкретный локализованный центр обработки данных, центы данных в облаке могут быть разбросаны по разным регионам, что расширяет поверхность атаки. Злоумышленники, как правило, используют любую уязвимость, обнаруженную в коде, конфигурациях и развертываниях, что приводит к катастрофическим последствиям для организации.

Данные клиентов и другая конфиденциальная информация являются наиболее важными активами, которыми может обладать та или иная организация, и иногда конкурирующие компании могут использовать услуги киберпреступников, чтобы получить преимущество перед своими конкурентами. Обязанность корпораций состоит в том, чтобы удержать злоумышленников подальше от данных пользователей, используя сочетание самых современных технологий и опытных групп кибербезопасности.

Одна из распространенных ошибок, которую совершают организации, заключается в том, что они считают поставщика облачных услуг гарантом безопасность облачных данных. Большинство поставщиков облачных услуг работают по модели общей ответственности, которая отвечает лишь за обеспечение безопасности базовой инфраструктуры и сетевых компонентов. В то же время именно заказчик несет ответственность за безопасность приложений, серверов и других компонентов, которые он создает в облаке.

Рост удаленной работы и увеличивающаяся зависимость от облачных сервисов усилили важность эффективных стратегий безопасности облачных данных. Цель этой статьи — дать обзор проблем, с которыми сталкиваются организации при защите своих облачных данных, и представить исчерпывающий набор передовых методов, которые помогут справиться с этими сложными проблемами. Понимая риски и применяя соответствующие меры безопасности, предприятия могут защитить свою ценную информацию и сохранить доверие к облачной экосистеме [1-2].

## 1. Проблемы защиты облачных данных

Организации сталкиваются с множеством проблем, когда речь заходит о защите их облачных данных, и понимание этих проблем имеет решающее значение для разработки комплексной стратегии облачной безопасности. Некоторые из наиболее распространенных проблем включают в себя:

- Общая ответственность. Безопасность облачных вычислений часто основывается на модели совместной ответственности, при которой и поставщик облачных услуг (CSP), и заказчик несут ответственность за различные аспекты безопасности. Организации должны четко понимать свои обязанности в этой модели, чтобы гарантировать отсутствие пробелов в безопасности из-за неосведомленности или недопонимания.
- Утечки данных: растущая частота утечек данных является серьезной проблемой для компаний, хранящих конфиденциальную информацию в облаке. Злоумышленники могут использовать уязвимости в облачной инфраструктуре или приложениях для получения несанкционированного доступа к данным, что может привести к значительному финансовому и репутационному ущербу [3].
- Внутренние угрозы. Злонамеренные инсайдеры или скомпрометированные учетные записи внутри организации могут представлять значительный риск для безопасности облачных данных. Сотрудники или подрядчики, имеющие доступ к конфиденциальной информации, могут намеренно или непреднамеренно вызвать утечку данных, подвергая организацию потенциальным юридическим и финансовым последствиям.
- Соблюдение нормативных требований: организации должны соблюдать различные отраслевые нормативные акты и законы о защите данных, такие как GDPR, HIPAA или CCPA, при хранении и обработке данных в облаке. Несоблюдение требований может

привести к крупным штрафам и ущербу для репутации, поэтому компаниям необходимо обеспечить соответствие своих методов обеспечения безопасности в облаке применимым нормам.

- Отсутствие видимости и контроля. В облачной среде организации часто имеют ограниченную видимость своих данных и приложений, что затрудняет эффективный мониторинг и управление безопасностью. Отсутствие контроля может увеличить риск несанкционированного доступа, потери данных или других нарушений безопасности.

Осознавая эти проблемы и оперативно решая их, организации могут создать надежную стратегию облачной безопасности, которая защитит их ценные данные и сведет к минимуму риск инцидентов, связанных с безопасностью [4].

**2. Лучшие практики для защиты облачных данных**

Для эффективной защиты облачных данных и снижения рисков, связанных с проблемами, упомянутыми ранее, организациям следует применять многогранный подход, включающий следующие передовые методы:

- Рекомендуется установление и применение строгой политики контроля доступа, чтобы ограничить доступ к облачным данным и приложениям. Реализуйте принцип наименьших привилегий, гарантируя, что пользователи имеют только необходимые разрешения для выполнения своих рабочих функций. Используйте многофакторную аутентификацию (MFA), чтобы добавить дополнительный уровень безопасности в процесс аутентификации.
- Шифрование конфиденциальных данные как в состоянии покоя, так и во время передачи, чтобы защитить их от несанкционированного доступа. Используйте надежные алгоритмы шифрования и методы управления ключами, чтобы свести к минимуму риск утечки данных.
- Непрерывный мониторинг и аудит облачных сред для выявления потенциальных угроз безопасности, неправильных конфигураций или несанкционированного доступа. Внедряйте автоматизированные инструменты и решения для улучшения видимости и контроля над облачными активами.
- Безопасные резервные копии и планы аварийного восстановления: регулярное сохранение резервных копий важных данных и приложений, чтобы обеспечить быстрое восстановление в случае потери данных или инцидентов безопасности. Разработка и тестирование комплексного плана аварийного восстановления, в котором описаны шаги, которые необходимо предпринять в случае чрезвычайной ситуации.
- Обучение сотрудников методам и политикам безопасности. Проведение регулярных программ обучения и повышения осведомленности, чтобы информировать сотрудников о важности безопасности облачных данных, передовых методиках и организационных политиках. Это может помочь снизить риск внутренних угроз и способствовать развитию культуры безопасности в организации.
- Тесное сотрудничество с поставщиками облачных услуг для обеспечения соответствия требованиям безопасности. Взаимодействие с CSP, чтобы убедиться, что их меры безопасности соответствуют требованиям вашей организации и применимым нормам.

Регулярные оценки безопасности и аудиты вашего CSP для поддержания безопасной облачной среды.

- Внедрение надежного плана реагирования на инциденты. Разработка и поддержка всеобъемлющего плана реагирования на инциденты, в котором излагаются шаги, которые необходимо предпринять в случае нарушения безопасности или других инцидентов. Этот план должен включать четкие роли и обязанности, протоколы связи и процедуры сдерживания, искоренения и восстановления [5].

Применяя эти передовые методы, компании могут разработать надежную и упреждающую стратегию безопасности облачных данных, которая эффективно устраняет проблемы и риски, связанные с хранением конфиденциальной информации в облаке.

### 3. Рекомендации для дальнейших исследований

Поскольку облачные вычисления продолжают развиваться и возникают новые проблемы безопасности, необходимы дальнейшие исследования, чтобы улучшить наше понимание безопасности облачных данных. Некоторые потенциальные области для дальнейших исследований включают [6-7]:

- Изучение применения передовых методов искусственного интеллекта и машинного обучения: исследуйте использование технологий искусственного интеллекта (ИИ) и машинного обучения (МО) для обнаружения и устранения угроз в облачных средах. Эти передовые методы могут помочь автоматизировать идентификацию угроз и реагирование на них, улучшая общее состояние безопасности организации.
- Исследование влияния новых технологий: оцените влияние новых технологий, таких как квантовые вычисления, на методы шифрования и безопасности данных. Понимание того, как эти технологии могут нарушить текущие меры безопасности, поможет организациям подготовиться к будущим угрозам.
- Анализ эффективности различных платформ и сертификатов облачной безопасности. Оцените роль и эффективность различных платформ и сертификатов облачной безопасности в обеспечении защиты данных. Этот анализ может помочь организациям выбрать наиболее подходящие стандарты безопасности и лучшие практики для своих конкретных потребностей.
- Оценка роли государственных постановлений и политик: изучите влияние государственных постановлений и политик на безопасность облачных данных и то, как они могут повлиять на будущее отрасли. Понимание меняющейся нормативно-правовой базы имеет решающее значение для организаций, чтобы соответствовать требованиям и поддерживать безопасную облачную среду.

Проводя дальнейшие исследования в этих областях, предприятия и исследователи могут внести свой вклад в разработку более надежных и адаптивных стратегий безопасности облачных данных, обеспечивающих защиту ценной информации в постоянно меняющемся цифровом ландшафте.

### Вывод

Защита облачных данных — сложная и многогранная задача, требующая комплексного подхода для устранения различных рисков и угроз. Понимая проблемы, связанные с защитой

облачных данных, применяя передовой опыт и получая информацию о последних тенденциях и разработках в области безопасности, организации могут эффективно защищать свою ценную информацию и поддерживать доверие к облачной экосистеме.

По мере того, как облачные вычисления продолжают развиваться и приобретать все большее значение, для предприятий крайне важно оставаться активными в своем подходе к безопасности облачных данных. Это включает в себя не только внедрение лучших практик, изложенных в этой статье, но и формирование культуры осведомленности о безопасности в организации и участие в текущих исследованиях, чтобы опережать возникающие угрозы.

В конечном счете, уделение особого внимания безопасности облачных данных поможет организациям воспользоваться преимуществами облачных вычислений и свести к минимуму риски, связанные с хранением и обработкой конфиденциальной информации в облаке.

**Список литературы**

1. Krasov A. V., Shterenberg S. I. Methods for building a trusted environment in Unix operating systems based on the implementation of a digital watermark //2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). – IEEE, 2020. – С. 253-257.
2. Сахаров Д. В. и др. Разработка модели обеспечения отказоустойчивости сети передачи данных //Известия высших учебных заведений. Технология легкой промышленности. – 2016. – Т. 34. – №. 4. – С. 14-20.
3. Штеренберг С. И., Красов А. В. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки // Учредители: Санкт-Петербургский государственный университет промышленных технологий и дизайна. – №. 1. – С. 26-36.
4. Пестов И. Е. и др. Мониторинг информации инстансов облачной инфраструктуры //Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). – 2023. – С. 216-220.
5. Бугрова Е. С. и др. Анализ методов повышения отказоустойчивости облачной инфраструктуры средствами мониторинга и предсказания состояния компонентов //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 188-192.
6. Пестов И. Е., Христофоров Р. О., Швидкий А. А. Анализ подходов к разработке облачных сервисов //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 752-757.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру //Инновационные решения социальных, экономических и технологических проблем современного общества. – 2021. – С. 113-115.

**References**

1. Krasov A. V., Shterenberg S. I. Methods for building a trusted environment in Unix operating systems based on the implementation of a digital watermark //2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). – IEEE, 2020. – pp. 253-257.

2. Sakharov D. V. et al. Development of a model for ensuring the fault tolerance of a data transmission network // Izvestia of higher educational institutions. Light industry technology. 2016. - T. 34. - No. 4. - pp. 14-20.
3. Shterenberg S. I., Krasov A. V. Bulletin of St. Petersburg state university of technology and design. Series 1: Natural and technical sciences // Founders: St. Petersburg State University of Industrial Technologies and Design. – no. 1. - pp. 26-36.
4. Pestov I. E. et al. Monitoring of information of cloud infrastructure instances // Training of professional personnel in the master's program for the digital economy (PKM-2022). - 2023. - pp. 216-220.
5. Bugrova E. S. et al. Analysis of methods for increasing the fault tolerance of cloud infrastructure by means of monitoring and predicting the state of components // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 188-192.
6. Pestov I. E., Khristoforov R. O., Shvidkiy A. A. Analysis of approaches to the development of cloud services // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 752-757.
7. Pestov I. E., Kosheleva S. A. Attacks on cloud infrastructure // Innovative solutions to social, economic and technological problems of modern society. - 2021. - pp. 113-115.