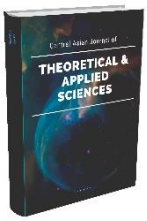

CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 04 Issue: 05 | May 2023 ISSN: 2660-5317
https://cajotas.centralasianstudies.org

Информационная Безопасность В «Облачных» Вычислительных Системах

Насриддинова П. Ф Асс., Юлдашев О. И.
Самаркандский филиал Ташкентского университета, информационных технологий имени Мухаммада ал-Хорезми

Received 4th Mar 2023, Accepted 6th Apr 2023, Online 23rd May 2023

Аннотации: Облачные вычисления стали неотъемлемой частью современной информационной инфраструктуры, обеспечивая удобный доступ к данным и вычислительным ресурсам через интернет. Однако, с расширением облачных технологий возникают и новые угрозы информационной безопасности. В этой статье мы рассмотрим основные аспекты информационной безопасности в облачных вычислениях и меры, которые можно принять для обеспечения безопасности данных.

Защита данных: Одним из главных аспектов безопасности в облачных вычислениях является защита данных. Важно обеспечить конфиденциальность, целостность и доступность данных, хранящихся и передаваемых в облаке. Для этого необходимо применять механизмы шифрования данных, как в покое, так и во время их передачи. Шифрование помогает предотвратить несанкционированный доступ к данным даже в случае их утечки или компрометации.

Управление доступом: Облачные системы часто имеют множество пользователей с различными уровнями доступа. Для обеспечения безопасности необходимо эффективно управлять аутентификацией и авторизацией пользователей. Сильные пароли, механизмы двухфакторной аутентификации и строгие политики паролей помогут предотвратить несанкционированный доступ. Кроме того, использование многоуровневых механизмов контроля доступа позволяет ограничить привилегии пользователей в соответствии с их ролями и обязанностями.

Физическая безопасность: Провайдеры облачных услуг должны обеспечивать физическую защиту своих центров обработки данных. Это включает меры контроля доступа, такие как системы видеонаблюдения, биометрическая идентификация и ограниченный доступ к серверным помещениям. Физическая безопасность является важным аспектом, поскольку она защищает оборудование и данные от угроз, связанных с несанкционированным доступом или физическими повреждениями.

Защита от атак: Облачные системы подвержены различным видам атак, таким как DDoS-атаки, вредоносное программное обеспечение и фишинг. Провайдеры облачных услуг должны принимать меры для обнаружения и предотвращения таких атак. Это включает использование средств мониторинга сетевой активности и трафика, установку брандмауэров и систем

обнаружения вторжений. Регулярное обновление программного обеспечения и применение патчей являются важными шагами для устранения уязвимостей и предотвращения эксплойтов.

Соответствие требованиям: Провайдеры облачных услуг должны соблюдать соответствующие стандарты безопасности и регулирования, такие как GDPR, HIPAA или PCI DSS, в зависимости от отрасли и видов данных, которые обрабатываются в облаке. Соблюдение этих требований помогает защитить конфиденциальность и права пользователей, а также предотвратить возможные санкции или ущерб для репутации компании.

Заключение: Информационная безопасность в облачных вычислениях является сложной и многогранной задачей. Защита данных, управление доступом, физическая безопасность, защита от атак и соблюдение требований являются основными аспектами, которые следует учитывать при разработке стратегии информационной безопасности в облачных вычислениях. Только путем принятия соответствующих мер безопасности можно обеспечить надежность и защиту данных в облачных средах.

Литература

1. XaaS Check 2010 – Status Quo und Trends im Cloud Computing. XaaS Check [Электронный ресурс]. – Режим доступа: http://www.xaas-check.eu/download.php?cat=00_Willkommen&file=2010-XaaS-CheckReport.pdf, свободный. Яз. нем. (дата обращения 04.12.2010).
2. Cloud Computing. Wikipedia, the free encyclopedia [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Cloud_computing, свободный. Яз. англ. (дата обращения 04.12.2010).
3. Сычев А.В. Теория и практика разработки современных клиентских веб-приложений. ИнтернетУниверситет Информационных Технологий [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/internet/thpdevweba/24/thpdevweba_24.html, свободный. Яз. рус. (дата обращения 04.12.2010).
4. Bernstein David, Ludvigson Erik, Sankar Krishna, Diamond Steve, Morrow Monique. Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability// IEEE Computer Society. – 2009.
5. GIAC Mission Statement. Global Information Assurance Certification [Электронный ресурс]. – Режим доступа: http://www.giac.org/overview/statement.php, свободный. Яз. англ. (дата обращения 04.12.2010).