УДК 004.056.57

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЁННЫХ И ОБЛАЧНЫХ СИСТЕМАХ: ПРОБЛЕМЫ И РЕШЕНИЯ

Ализода С.С.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Лихачевский Д.В. – к. т. н., доцент, декан ФКП

Аннотация. В статье рассматриваются основные угрозы безопасности в облачных и распределенных системах, включая утечку данных, атаки на учетные записи и DDoS-атаки. Проанализированы методы защиты, такие как шифрование, многофакторная аутентификация и мониторинг сетевого трафика. Особое внимание уделено перспективным направлениям, включая квантовую криптографию и автоматизацию кибербезопасности.

Ключевые слова: облачная безопасность, кибератаки, управление доступом, мониторинг, шифрование.

Введение. С развитием облачных технологий и распределённых вычислительных систем компании и пользователи получают доступ к удобным и масштабируемым сервисам. Однако наряду с преимуществами облачных решений возникают серьёзные проблемы безопасности, такие как утечка данных, несанкционированный доступ и атаки на инфраструктуру. В данной статье рассматриваются основные проблемы обеспечения безопасности в распределённых и облачных системах, а также предлагаются решения для их минимизации.

Основная часть. Распределённые и облачные системы подвержены ряду угроз, связанных с их архитектурными особенностями и методами хранения и обработки данных. Основные проблемы включают:

1 Утечка и компрометация данных – так как данные хранятся на серверах провайдеров облачных услуг, существует риск несанкционированного доступа, утечки или кражи конфиденциальной информации.

2 Отказ в обслуживании (DDoS-атаки) – злоумышленники могут перегрузить облачные сервисы, затрудняя доступ к ним для легитимных пользователей.

3 Уязвимости многопользовательской среды – виртуализация и совместное использование серверных мощностей могут привести к несанкционированному доступу к данным других пользователей.

4 Несанкционированный доступ и атаки на учетные записи – использование слабых паролей или недостаточная защита аутентификации может привести к компрометации учётных данных.

5 Отсутствие прозрачности у облачных провайдеров – пользователи зависят от мер безопасности, реализованных провайдером, и не всегда имеют полный контроль над защитой своих данных.

6 Законодательные и нормативные риски – компании, использующие облачные сервисы, должны соблюдать законы о защите данных, такие как GDPR и HIPAA, что усложняет администрирование.

Для обеспечения безопасности в облачных и распределённых системах применяются следующие методы и технологии:

1 Шифрование данных:

– шифрование в процессе передачи (TLS, SSL) защищает данные при обмене между клиентами и серверами;

– шифрование при хранении (AES, RSA) предотвращает несанкционированный доступ к данным в облаке;

– гомоморфное шифрование позволяет производить вычисления над зашифрованными данными без их расшифровки.

2 Многофакторная аутентификация (MFA): использование дополнительных факторов аутентификации (одноразовые коды, биометрия, аппаратные ключи) снижает риск компрометации учётных данных.

3 Управление доступом (IAM):

– политики контроля доступа (RBAC, ABAC) позволяют ограничивать права пользователей в облачных системах;

– реализация принципа наименьших привилегий снижает риски несанкционированного доступа.

4 Мониторинг и реагирование на инциденты:

– системы обнаружения и предотвращения вторжений (IDS/IPS) анализируют сетевой трафик и выявляют подозрительную активность;

– SIEM-системы (Security Information and Event Management) собирают и анализируют логи безопасности для выявления аномалий;

– автоматизация реагирования на инциденты (SOAR) ускоряет обработку угроз.

5 Защита виртуальных машин и контейнеров:

– сегментация сети ограничивает взаимодействие между виртуальными машинами и предотвращает боковые атаки;

– сканирование образов контейнеров помогает выявить уязвимости в контейнеризированных приложениях;

– политики безопасности Kubernetes обеспечивают контроль за развертыванием облачных сервисов.

6 Резервное копирование и аварийное восстановление:

– автоматизированные резервные копии обеспечивают защиту от потери данных при сбоях или атаках;

– размещение резервных копий в географически распределённых хранилищах повышает отказоустойчивость.

7 Безопасность API и облачных сервисов:

– использование OAuth 2.0 и OpenID Connect для безопасной аутентификации;

– мониторинг API-запросов и ограничение доступа к критически важным функциям.

8 Обучение пользователей и сотрудников:

– проведение тренингов по кибербезопасности снижает риск атак, связанных с социальной инженерией;

– создание политик безопасности, направленных на защиту корпоративных данных.

С развитием облачных технологий появляются новые методы защиты. Основные перспективные направления включают:

– искусственный интеллект и машинное обучение для анализа аномалий и автоматического выявления угроз;

– конфиденциальные вычисления (Confidential Computing) – использование аппаратных решений для безопасной обработки данных в облаке;

– квантовая криптография – создание новых алгоритмов защиты, устойчивых к атакам квантовых компьютеров;

– децентрализованные идентификационные системы – использование блокчейна для управления цифровыми удостоверениями.

Заключение. Безопасность распределённых и облачных систем требует комплексного подхода. Использование современных технологий шифрования, управления доступом, мониторинга и автоматизированного реагирования позволяет снизить риски атак. Однако

обеспечение кибербезопасности – это непрерывный процесс, требующий адаптации к новым угрозам и постоянного совершенствования стратегий защиты. Организации, активно инвестирующие в безопасность облачных решений, смогут защитить свои данные и минимизировать потенциальные угрозы.

Список литературы

1. *Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2022.*
2. *Shinder, D., Shinder, T. Cloud Security Handbook: Best Practices for Secure Cloud Computing. Packt, 2021.*
3. *Krutz, R. L., Vines, R. D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, 2010.*
4. *National Institute of Standards and Technology (NIST). Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing. Gaithersburg, MD: NIST, U.S. Department of Commerce.*
5. *GDPR (General Data Protection Regulation) [Electronic resource]. – Available at: https://gdpr-info.eu/. – Accessed: March 20, 2025.*
6. *OWASP. Cloud Security Project [Electronic resource]. – Available at: https://owasp.org/www-project-cloud-security/. – Accessed: March 20, 2025.*
7. *Cloud Security Alliance (CSA) [Electronic resource]. – Available at: https://cloudsecurityalliance.org. – Accessed: March 20, 2025.*

UDC 004.056.57

SECURITY TECHNOLOGIES IN DISTRIBUTED AND CLOUD SYSTEMS: PROBLEMS AND SOLUTIONS

Alizoda S.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Likhachevsky D.V. – Cand. of Sci., Associate Professor, Dean of FCAD

Annotation. The article discusses key security threats in cloud and distributed systems, including data breaches, account hijacking, and DDoS attacks. It analyzes security methods such as encryption, multi-factor authentication, and network traffic monitoring. Special attention is given to future directions, including quantum cryptography and cybersecurity automation.

Keywords: cloud security, cyberattacks, access management, monitoring, encryption.