Лешуков Иван Сергеевич, магистрант,
Кубанский Государственный Университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ СЕРВИСАХ: ЗАЩИТА ДАННЫХ И ПРИЛОЖЕНИЙ

Аннотация. В статье рассматриваются ключевые аспекты информационной безопасности в облачных сервисах. Исследование подтверждает, что защита данных требует комплексного подхода, включающего шифрование, контроль доступа и системы мониторинга. Особое внимание уделяется технологическим и управленческим мерам, а также распределению ответственности между клиентом и провайдером.

Ключевые слова: Информационная безопасность, облачные сервисы, шифрование, кибератаки, управление рисками, соответствие требованиям.

Современный этап цифровой трансформации характеризуется массовым переходом организаций на облачные технологии. По данным исследований, более 80% компаний уже используют облачные сервисы в своей деятельности [1]. Однако вместе с преимуществами облачных решений – гибкостью, масштабируемостью и экономической эффективностью – возникают серьезные риски в области информационной безопасности. Последние статистические данные показывают, что количество инцидентов безопасности в облачной среде выросло на 107% с начала 2024 года, а средний ущерб от одного инцидента превышает 4 миллиона долларов.

Основные угрозы безопасности в облачных средах можно разделить на несколько категорий:

- Внешние угрозы: целенаправленные кибератаки, DDoS-воздействия и эксплуатация уязвимостей программного обеспечения.
- Внутренние угрозы: ошибки конфигурации, которые, по данным экспертов, становятся причиной 85% всех инцидентов.
- Системные угрозы: уязвимости мультитенантной среды и проблемы безопасности API [4].

Ярким примером последствий недостаточной защиты облачных сервисов стала утечка данных Capital One в 2019 году. Инцидент, вызванный ошибкой конфигурации межсетевого экрана, привел к компрометации персональных данных более 100 миллионов клиентов и повлек за собой штрафные санкции на сумму 200 миллионов долларов [3].

Для эффективного противодействия угрозам применяется комплекс технических и организационных мер:

Технические меры:

- Шифрование данных при хранении (AES-256) и передаче (TLS/SSL).
- Системы управления доступом с многофакторной аутентификацией.
- SIEM-системы для мониторинга безопасности в режиме реального времени.

Организационные меры:

- Регулярные аудиты и обучение сотрудников.
- Внедрение практик DevSecOps.
- Четкое распределение ответственности между клиентом и провайдером [2].

В модели IaaS клиент несет ответственность за безопасность данных, приложений и операционных систем, в то время как провайдер обеспечивает защиту физической инфраструктуры. В моделях PaaS и SaaS зона ответственности провайдера расширяется, охватывая также платформу и программное обеспечение.

Перспективы развития связаны с дальнейшей автоматизацией процессов защиты, внедрением технологий искусственного интеллекта для обнаружения угроз и развитием стандартов безопасности. Особое внимание уделяется вопросам соответствия международным и отраслевым регуляторным требованиям, таким как GDPR, ISO 27001 [5].

Комплексный подход к обеспечению безопасности в облачных средах, сочетающий технические решения, организационные меры и четкое распределение ответственности, позволит организациям в полной мере использовать преимущества облачных технологий, минимизируя сопутствующие риски.

Список литературы:

1. Егоров П. С. Облачные технологии и информационная безопасность. – М.: Альфа-Пресс, 2020. – 240 с.

2. Жуков А. В. Методы шифрования для защиты облачных данных. – СПб.: Наука, 2022. – 352 с.

3. Иванов К. Л. Анализ и противодействие кибератакам на облачные сервисы. – М.: Интуит, 2023. – 296 с.

4. Козлов Д. Р. Комплексное управление рисками информационной безопасности в облаках. – М.: КноРус, 2021. – 312 с.

5. Лебедев М. Ф. Нормативное регулирование и соответствие требованиям в области облачной безопасности. – М.: Дело, 2020. – 264 с.

6. Петров В. Г. Информационная безопасность облачных вычислений. – М.: Форум, 2022. – 280 с.

7. Сидоров А. И. Шифрование и защита информации в облачных сервисах. – М.: Риор, 2023. – 336 с.