УДК 004.62

ТЕХНИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

К.А. Скалозуб, С.Н. Нестеренков, Е.В. Бегляк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются основные технические аспекты защиты данных в облачных вычислениях. Описаны ключевые угрозы безопасности, такие как утечки данных, атаки на инфраструктуру и компрометация учетных записей, которые могут привести к серьезным последствиям для организаций и пользователей. Анализируются современные технологии защиты.

включая шифрование, многофакторную аутентификацию, модели контроля доступа и технологии защиты данных во время передачи и хранения. Подчеркивается важность интеграции средств защиты в облачные системы для обеспечения их надежности, повышения уровня безопасности и соответствия современным стандартам. Внедрение эффективных методов защиты данных является необходимым условием для минимизации рисков и обеспечения доверия пользователей к облачным сервисам и приложениям, что актуально в условиях быстрого роста объемов данных и увеличения киберугроз.
Ключевые слова: облачные вычисления; защита данных; кибербезопасность; шифрование; аутентификация; контроль доступа; утечки данных; атаки на инфраструктуру; компрометация учетных записей; технологии защиты.

TECHNICAL ASPECTS OF DATA PROTECTION IN CLOUD COMPUTING

K.A. Skalozub, S.N. Nesterenkov, E.V. Begliak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the main technical aspects of data protection in cloud computing. It describes key security threats, such as data leaks, infrastructure attacks, and account compromises, which can lead to serious consequences for organizations and users. Modern protection technologies are analyzed, including encryption, multi-factor authentication, access control models, and data protection technologies during transmission and storage. The importance of integrating protective measures into cloud systems is emphasized to ensure their reliability, enhance security levels, and comply with modern standards. Implementing effective data protection methods is essential for minimizing risks and ensuring user trust in cloud services and applications, which is particularly relevant in the context of rapid data growth and increasing cyber threats.
Keywords: cloud computing; data protection; cybersecurity; encryption; authentication; access control; data leaks; infrastructure attacks; account compromise; protection technologies.

Введение

С развитием облачных вычислений увеличивается объем обрабатываемых и хранящихся данных. Это создает новые вызовы для обеспечения безопасности, так как данные, находящиеся в облаке, могут быть уязвимы для различных угроз. Защита данных становится приоритетной задачей как для поставщиков облачных услуг, так и для их клиентов. В данной статье рассматриваются ключевые угрозы безопасности и современные технологии защиты данных в облачных вычислениях, а также значимость интеграции средств защиты для обеспечения надежности и доверия к облачным сервисам.

Угрозы безопасности

Облачные вычисления подвержены ряду угроз, среди которых:

1. Утечки данных. Данные могут быть случайно или намеренно раскрыты третьим лицам, что приводит к финансовым потерям и потере репутации. Утечки могут происходить из-за недостатков в системе безопасности, человеческого фактора или недобросовестных действий сотрудников.

2. Атаки на инфраструктуру. Хакеры могут целенаправленно атаковать облачные сервисы, используя уязвимости в системах безопасности. Это может включать DDoS-атаки, направленные на перегрузку серверов или атаки на программное обеспечение, использующее уязвимости.

3. Компрометация учетных записей. Неавторизованный доступ к учетным записям может привести к манипуляциям с данными и их утечке. Использование слабых паролей и отсутствие многофакторной аутентификации значительно увеличивают риски.

4. Недостаточная безопасность облачной инфраструктуры. Многие организации полагаются на облачных провайдеров для обеспечения безопасности, однако недостаточная защита на уровне инфраструктуры может привести к серьезным последствиям. Это включает в себя отсутствие шифрования данных и недостаточные меры по управлению доступом.

5. Неправильная конфигурация облачных ресурсов. Ошибки в настройках облачных сервисов могут привести к уязвимостям. Например, неправильно настроенные разрешения могут позволить доступ к данным неавторизованным пользователям.

Технологии защиты данных

Для борьбы с угрозами применяются различные технологии и методы защиты. Шифрование данных, как в процессе передачи, так и в состоянии покоя, является основным методом защиты. Оно защищает данные от несанкционированного доступа, даже если они будут перехвачены. Современные методы шифрования, такие как AES (Advanced Encryption Standard), обеспечивают высокий уровень безопасности и могут использоваться для защиты как файлов, так и сетевых соединений.

Использование многофакторной аутентификации (MFA) значительно повышает уровень безопасности. MFA требует от пользователей предоставления нескольких форм идентификации, что затрудняет доступ злоумышленников. Например, сочетание пароля и одноразового кода, отправленного на мобильный телефон, делает учетные записи более защищенными.

Эффективные модели контроля доступа позволяют ограничить доступ к данным только авторизованным пользователям. Это может быть реализовано через ролевое управление доступом (RBAC) или атрибутное управление доступом (ABAC). Использование таких моделей помогает применять принцип наименьших привилегий, что снижает риски утечек данных.

Системы виртуальных частных сетей (VPN) и протоколы защищенной передачи данных, такие как SSL/TLS, помогают защитить данные во время их передачи через интернет. Эти технологии обеспечивают шифрование и аутентификацию, что позволяет защитить данные от перехвата и несанкционированного доступа.

Регулярный мониторинг и аудит безопасности помогают выявлять и устранять уязвимости. Использование систем обнаружения вторжений (IDS) и систем управления информацией и событиями безопасности (SIEM) позволяет отслеживать подозрительную активность и реагировать на инциденты в реальном времени.

Заключение

Защита данных в облачных вычислениях является сложной, но необходимой задачей, требующей внимания со стороны всех участников процесса. Внедрение современных технологий защиты данных, таких как шифрование, многофакторная аутентификация и модели контроля доступа, поможет минимизировать риски и повысить уровень доверия пользователей к облачным сервисам. В условиях быстрого роста объемов данных и увеличения киберугроз эффективная защита данных становится ключевым элементом успешного функционирования облачных решений. Организации должны быть готовы адаптироваться к изменяющимся угрозам и постоянно улучшать свои стратегии защиты данных.

Список использованных источников

1. Самокиш А.В. (2017) Облачные технологии. *Экономика и социум*. 1–4.
2. Никульчев Е.В., Лукьянчиков О.И., Ильин Д.Ю. (2019) *Облачные технологии*. Москва, Издательство «РТУ МИРЭА».
3. Иванов П.В. (2025) *Менеджмент: методы принятия управленческих решений*. Москва. Издательство «Юрайт».
4. Исаев Е.А., Думский Д.В., Самодуров В.А., Корнилов В.В. (2015) Обеспечение информационной безопасности облачных вычислений. *Математическая биология и биоинформатика*. 571–577.
5. Сафонов В.А. (2024) Исследование уязвимостей и методов защиты данных в облачных информационных хранилищах. *Актуальные исследования*. 1–5.

References

1. Samokish A.V. (2017) Cloud technologies. 1–4 (in Russian).
2. Nikilchev E.V., Lukyanchikov O.I., Iluin D.Yu. (2019) *Cloud technologies*. Moscow. RTU MIREA Publishing House (in Russian).
3. Ivanov P.V. (2025) *Management: methods of making management decisions*. Moscow, Yurait Publishing House (in Russian).
4. Isaev E.A., Dumsky D.V., Samodurov V.A., Kornilov V.V. (2015) Ensuring information security of cloud computing. *Mathematical biology and bioinformatics*. 571–577 (in Russian).
5. Safonov V.A. (2024) Study of vulnerabilities and methods of data protection in cloud information storages. *Current researches*. 1–5 (in Russian).

Сведения об авторах

Скалозуб К.А., студент кафедры электронных вычислительных машин, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», seniaskalozub6@gmail.com.
Нестеренков С.Н., канд. техн. наук, доцент кафедры программного обеспечения информационных технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.nesterenkov@bsuir.by.
Бегляк Е.В., магистрант, ассистент кафедры вычислительных методов и программирования, инженер-программист 1 категории отдела сетевых технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», katarina@bsuir.by.

Information about the authors

Skalazub K., Student of the Department of Electronic Computing Machines, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kseniaskalozub6@gmail.com.
Nesterenkov S., Cand. Sc. (Tech.), Associate Professor of the Department of Information Technology Software, Educational Institution "Belarusian State University of Informatics and Radioelectronics", s.nesterenkov@bsuir.by.
Begliak E.V., Master's student, Assistant at the Department of Computational Methods and Programming, 1st category Software Engineer of the Network Technologies Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", katarina@bsuir.by.