Нижлукченко И.Д. Безопасность в облаке: как защитить свои данные в облачных сервисах. советы по выбору облачных провайдеров и настройке облачных сервисов для обеспечения безопасности данных // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 6(44) с. 95–100

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

БЕЗОПАСНОСТЬ В ОБЛАКЕ: КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ В ОБЛАЧНЫХ СЕРВИСАХ. СОВЕТЫ ПО ВЫБОРУ ОБЛАЧНЫХ ПРОВАЙДЕРОВ И НАСТРОЙКЕ ОБЛАЧНЫХ СЕРВИСОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В статье "Безопасность в облаке: как защитить свои данные в облачных сервисах" освещаются ключевые аспекты и стратегии обеспечения безопасности цифровой информации в условиях широкого использования облачных технологий. В условиях быстрого роста объемов генерируемых данных и их ценности, вопросы конфиденциальности, целостности и доступности информации становятся всё более актуальными. Статья представляет собой комплексный обзор методов защиты данных, начиная с выбора надежных облачных провайдеров, настройки облачных сервисов, до проведения регулярных аудитов и мониторинга системы безопасности. Особое внимание уделяется не только техническим, но и организационным аспектам защиты данных, подчеркивая важность комплексного подхода, который включает в себя обучение персонала, разработку и внедрение политик безопасности. Статья подчеркивает, что в современных условиях обеспечение безопасности данных в облаке является непрерывным процессом, требующим от организаций гибкости, постоянного обучения и адаптации к изменяющемуся ландшафту угроз.

Ключевые слова: Безопасность данных, облачные сервисы, облачные провайдеры, шифрование данных, аудит безопасности, мониторинг безопасности, настройка облачных сервисов, многофакторная аутентификация, резервное копирование, непрерывность бизнеса, кибербезопасность, защита конфиденциальности, целостность данных, доступность данных, управление угрозами, стандарты безопасности данных, GDPR, HIPAA, обучение персонала, культура безопасности.

SECURITY IN THE CLOUD: HOW TO PROTECT YOUR DATA IN CLOUD SERVICES. TIPS ON CHOOSING CLOUD PROVIDERS AND CONFIGURING CLOUD SERVICES TO ENSURE DATA SECURITY

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

The article "Security in the cloud: how to protect your data in cloud services" highlights key aspects and strategies for ensuring the security of digital information in the context of widespread use of cloud technologies. With the rapid growth of the volume of data generated and its value, issues of confidentiality, integrity and accessibility of information are becoming increasingly relevant. The article provides a comprehensive overview of data protection methods, from choosing reliable cloud providers, configuring cloud services, to conducting regular audits and

monitoring the security system. Special attention is paid not only to the technical, but also to the organizational aspects of data protection, emphasizing the importance of an integrated approach that includes staff training, development and implementation of security policies. The article emphasizes that in modern conditions, ensuring data security in the cloud is an ongoing process that requires organizations to be flexible, constantly learning and adapting to the changing threat landscape.

Keywords: Data security, cloud services, cloud providers, data encryption, security audit, security monitoring, configuring cloud services, multi-factor authentication, backup, business continuity, cybersecurity, privacy protection, data integrity, data availability, threat management, data security standards, GDPR, HIPAA, staff training, culture security.

В эпоху цифровизации, облако стало ключевым элементом в хранении и обработке данных для организаций и индивидуальных пользователей. Однако с ростом его популярности возрастает и количество угроз безопасности данных. Поэтому понимание методов защиты информации в облаке и правильный выбор облачных провайдеров становится критически важным для обеспечения конфиденциальности, целостности и доступности данных.

Защита данных в облаке представляет собой многоаспектный процесс, основанный на глубоком понимании как технологических, так и человеческих факторов, способных повлиять на безопасность информации. В рамках комплексного подхода к безопасности данных ключевым является осознание того, что угрозы могут исходить как извне, так и изнутри организации, а также понимание того, как технические и организационные меры могут работать вместе для минимизации рисков.

На начальном этапе аудит существующих систем безопасности позволяет выявить слабые места и уязвимости в текущей архитектуре безопасности. Это исследование охватывает как физические, так и цифровые аспекты защиты данных, включая анализ методов аутентификации, шифрования, а также процедур восстановления после сбоев. Основываясь на результатах аудита, разрабатывается стратегия безопасности, предусматривающая внедрение современных технологий защиты данных и обновление устаревших систем.[1]

Следующим шагом является определение критериев выбора облачного провайдера, что включает в себя анализ его политики безопасности, возможностей по шифрованию данных и предложений по резервному копированию. Ключевым моментом здесь является выбор провайдера, способного обеспечить не только высокий уровень защиты данных, но и соответствие международным стандартам и нормативным требованиям в области защиты данных.

Организационные меры включают в себя разработку политик и процедур, регулирующих доступ к данным, их использование и распределение. Важно обучать сотрудников основам кибергигиены, правилам работы с чувствительной информацией и способам распознавания фишинговых атак. Также критически важным является введение политики регулярного обновления программного обеспечения и использования современных антивирусных решений для защиты от вредоносного программного обеспечения и других угроз.

Интеграция технических и организационных мер требует не только первоначальных инвестиций в инфраструктуру безопасности, но и постоянного мониторинга ситуации в области кибербезопасности, адаптации к новым угрозам и уязвимостям. Таким образом, комплексный подход к безопасности данных в облаке предполагает непрерывное взаимодействие между технологиями, процессами и людьми, направленное на защиту самого ценного актива любой организации — ее данных.

Выбор облачного провайдера является одним из наиболее значимых решений, влияющих на безопасность данных. Этот процесс начинается с тщательного анализа потребностей организации в области хранения, обработки и управления данными. Важно оценить, какие виды данных будут храниться в облаке, и какие требования к безопасности эти данные предъявляют.[4] Это помогает определить, какие функции безопасности должен предлагать провайдер, чтобы соответствовать как операционным, так и нормативным требованиям.

Ключевым аспектом является изучение политик безопасности и практик облачного провайдера, включая методы шифрования, которые он использует для защиты данных в покое и во время передачи. Шифрование становится критически важной защитой, поскольку оно обеспечивает, что даже в случае несанкционированного доступа данные останутся недоступными для злоумышленников.

Далее, оценка механизмов аутентификации и контроля доступа, предлагаемых провайдером, позволяет убедиться, что только авторизованные пользователи смогут получить доступ к данным. Это включает в себя поддержку многофакторной аутентификации, ролевого доступа и других современных методов управления идентификацией и доступом.

Важно также учитывать политику и механизмы резервного копирования и восстановления данных, предлагаемые провайдером. В случае кибератак, технических сбоев или других чрезвычайных ситуаций, возможность быстро восстановить данные является ключевым аспектом поддержания непрерывности бизнеса.

Помимо технических аспектов, в процессе выбора провайдера важно учитывать его репутацию, опыт работы на рынке и отзывы других клиентов. Не менее важным является и его способность соответствовать местным и международным нормативным требованиям в области защиты данных, таким как GDPR или HIPAA, что особенно актуально для организаций, работающих в регулируемых отраслях.

В итоге, выбор облачного провайдера должен основываться на глубоком понимании как технических возможностей провайдера в области обеспечения безопасности данных, так и его способности соответствовать требованиям бизнеса и законодательства. Это стратегическое решение требует комплексного подхода и должно включать в себя как тщательную оценку текущих и будущих потребностей в облачных услугах, так и глубокий анализ предлагаемых провайдером решений по обеспечению безопасности.

Настройка облачных сервисов для обеспечения безопасности данных требует внимательного подхода и глубокого понимания как функционала облачных платформ, так и потенциальных угроз. Этот процесс начинается с анализа предоставляемых облачной платформой инструментов и возможностей по управлению доступом, шифрованию, аудиту и мониторингу. Важно настроить эти инструменты таким образом, чтобы максимально усилить защиту данных, при этом сохраняя баланс между безопасностью и удобством использования для конечных пользователей.

Применение принципа наименьших привилегий при настройке учетных записей пользователей является фундаментальным аспектом защиты данных в облаке. Это означает предоставление пользователям таких прав доступа, которые строго соответствуют их ролям и задачам, минимизируя тем самым возможность несанкционированного доступа к чувствительной информации. В дополнение к этому, регулярное обновление паролей и

использование многофакторной аутентификации значительно увеличивают уровень защиты учетных записей от взлома.

Шифрование данных, как в состоянии покоя, так и в процессе их передачи, становится неотъемлемой частью стратегии безопасности. Настройка шифрования должна проводиться с учетом специфики данных и требований к их защите. Облачные платформы обычно предлагают различные опции шифрования, позволяя выбрать наиболее подходящие в зависимости от уровня требуемой безопасности и производительности.

Кроме того, важным аспектом настройки является настройка процессов резервного копирования и восстановления данных. Это не только способ защиты от потери данных в случае технических сбоев или кибератак, но и ключевой элемент стратегии обеспечения непрерывности бизнеса. Настройка резервного копирования должна включать определение частоты создания резервных копий, а также выбор надежных и безопасных мест их хранения.

Настройка систем мониторинга и аудита играет важную роль в своевременном выявлении и реагировании на инциденты безопасности.[2] Эти системы должны быть сконфигурированы таким образом, чтобы обеспечить непрерывный анализ активности в облачной инфраструктуре, выявляя подозрительные действия и аномалии, которые могут указывать на попытки несанкционированного доступа или другие угрозы безопасности.

В целом, настройка облачных сервисов для обеспечения безопасности данных - это процесс, требующий не только технических знаний, но и понимания текущего ландшафта угроз и лучших практик в области кибербезопасности.

В контексте обеспечения безопасности данных в облаке, регулярный аудит и мониторинг становятся неотъемлемой частью стратегии защиты. Эти процессы позволяют не только выявлять и устранять уязвимости в системе безопасности, но и адаптироваться к постоянно меняющемуся ландшафту угроз.

Регулярный аудит системы безопасности облачных сервисов предполагает всестороннюю проверку всех аспектов защиты данных, включая анализ эффективности применяемых методов шифрования, политик доступа, механизмов аутентификации и инструментов мониторинга. В рамках аудита осуществляется также проверка соответствия действующим стандартам и регуляторным требованиям в области защиты данных. Этот процесс позволяет идентифицировать потенциальные уязвимости и разработать план их устранения, повышая тем самым общий уровень безопасности облачной инфраструктуры.

Мониторинг активности в облачных сервисах является постоянным процессом, который позволяет в реальном времени отслеживать события безопасности, анализировать трафик данных и выявлять подозрительные действия, которые могут указывать на попытки несанкционированного доступа, вредоносные атаки или внутренние угрозы. Современные системы мониторинга обладают возможностью автоматического распознавания аномалий в поведении пользователей и приложений, что позволяет своевременно реагировать на потенциальные угрозы и предотвращать инциденты безопасности.

Ключевым моментом является то, что регулярный аудит и мониторинг не являются разовыми мероприятиями, а представляют собой непрерывный процесс. Это требует от организаций не только наличия квалифицированных специалистов в области кибербезопасности, но и использование передовых инструментов и технологий для анализа и управления безопасностью.[3] Регулярное обновление политик безопасности, а также

адаптация к новым угрозам и изменениям в регуляторной среде, позволяет поддерживать высокий уровень защиты данных в облаке.

Таким образом, регулярный аудит и мониторинг служат важным звеном в цепочке обеспечения безопасности данных в облаке, позволяя организациям не только обнаруживать и устранять уязвимости, но и прогнозировать потенциальные угрозы, обеспечивая тем самым надежную защиту своих цифровых активов.

В заключение, безопасность данных в облачных сервисах остается важнейшей задачей для организаций всех размеров и сфер деятельности. В современном мире, где цифровизация проникает во все аспекты нашей жизни, и где объемы данных растут с каждым днем, вопросы защиты информации становятся критически важными.[5] Принятие комплексного подхода к безопасности, который включает в себя тщательный выбор облачных провайдеров, настройку облачных сервисов, регулярный аудит и мониторинг, позволяет создать надежную систему защиты данных. Это не только обеспечивает сохранность и конфиденциальность важной информации, но и способствует поддержанию доверия клиентов и партнеров, что является неотъемлемым аспектом успешного ведения бизнеса.

С другой стороны, необходимо осознавать, что процесс обеспечения безопасности данных в облаке – это непрерывная активность, требующая постоянного внимания, обучения и адаптации к изменяющемуся ландшафту угроз. В этом контексте важна не только технологическая составляющая, но и человеческий фактор, включая обучение сотрудников и формирование культуры безопасности внутри организации. В конечном итоге, безопасность облачных данных становится совместной ответственностью провайдеров облачных услуг и их клиентов, требующей скоординированных усилий, передовых технологий и стратегического планирования для обеспечения защиты цифровых активов в долгосрочной перспективе.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе//Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO//Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux//Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.