УДК 004.65.657

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ХРАНИЛИЩ

Акбаржонов А.Б., Эльмуродов Ш.Ш.

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

Научный руководитель: Асадчая Э.В. – ассистент кафедры ПИКС

Аннотация. В данной статье рассматриваются основные угрозы безопасности облачных хранилищ, такие как утечки данных, атаки злоумышленников, несанкционированный доступ к данным и др. Также описываются основные меры безопасности, которые могут быть приняты для защиты облачных хранилищ данных.

Ключевые слова: безопасность, шифрование, авторизация.

Введение. В современном мире облачные хранилища занимают все более значимую роль в сфере хранения информации. Они позволяют быстро и удобно сохранять и обмениваться данными, их использование не требует больших затрат на оборудование и техническую поддержку. Однако вопрос безопасности облачных хранилищ остается актуальным, т.к. хранение в облаке подразумевает передачу данных по сети, что может повлечь за собой угрозы для конфиденциальности информации.

Основная часть. В наши дни многие большие компании считают облачную инфраструктуру более безопасной, но при этом меньшая часть предпринимают дополнительные защитные меры. Например, 61% клиентов прибегают к шифрованию данных, 52% ведут политику управления идентификацией и доступом к информационным системам, а 48% — проводят регулярные проверки систем.

Областные хранилища данных являются ключевым элементом информационной инфраструктуры любой крупной компании или организации. Они предназначены для хранения всех важных данных, от финансовой информации до интеллектуальной собственности, и играют важную роль в обеспечении безопасности и конфиденциальности этих данных.

Однако несмотря на это областные хранилища являются центральным элементом информационной инфраструктуры, они также могут стать объектом атак со стороны злоумышленников. Нарушители могут использовать различные методы для получения несанкционированного доступа к хранилищам, в том числе использование вредоносных программ или физическое взлом зданий [1].

Поэтому, для обеспечения безопасности областных хранилищ, необходимо применять комплексный подход, который включает в себе четыре меры следующего содержания:

1 **Криптографическая защита данных.** Криптографическая защита данных является одним из самых эффективных методов защиты данных в облачных хранилищах данных. Это включает в себя использование криптографических алгоритмов для шифрования данных в хранилищах, что делает их недоступными для несанкционированного доступа.

2 **Физическая защита.** Физическая защита является не менее важной для облачных хранилищ данных. Это включает в себя использование безопасности зданий, систем видеонаблюдения и контроля доступа, а также радиочастотных идентификаторов для определения местонахождения сотрудников и пользователей.

3 **Применение многофакторной аутентификации.** Многофакторная аутентификация является дополнительной мерой безопасности, которая усиливает процесс аутентификации при входе в систему. Этот метод требует от пользователей предоставления нескольких форм идентификации, таких как пароль, отпечаток пальца или смарт-карты, прежде чем они получат доступ к хранилищу.

4 Аудит и мониторинг безопасности. Важным элементом обеспечения безопасности облачных хранилищ является проведение аудита и мониторинга безопасности системы. Периодические проверки на наличие уязвимостей и аномалий помогут выявить подозрительное поведение или обнаружить возможные угрозы безопасности.

Несмотря на то, что сегодня мы имеем значительно более широкий набор инструментов для обеспечения безопасности, чем прежде, улучшения облачных систем безопасности все ещё продолжается. В некоторых случаях для вывода на рынок той или иной технологии, помогающей решить новую задачу, проходит некоторое время, даже несмотря на то, что она уже разработана. Вот некоторые из таких новейших технологий: данные со встроенной защитой (самозащищенные данные) и доверенные мониторы.

Самозащищенные данные (*self-protecteddata*) – это зашифрованные данные, в которые интегрирован механизм обеспечения безопасности. Такой механизм включает в себя набор правил, которым может или не может удовлетворять среда, в которой находятся самозащищенные данные. При попытке доступа к этим данным, механизм проверяет среду на безопасность и раскрывает их, только если среда является безопасной [2–3].

Заключение. При рассмотрении всех подходов и мер, применяемых облачными хранилищами, было выявлено что обеспечение безопасности облачных хранилищ данных является необходимым для защиты конфиденциальности и целостности важной информации организации. Применение комплексного подхода, включающего криптографическую защиту, физическую защиту, многофакторную аутентификацию и аудит безопасности, позволит минимизировать риски нарушения безопасности областных хранилищ данных.

Список литературы

1. Архипенков, С. Хранилища данных. От концепции до внедрения / С. Архипенков, Д. Голубев, О. Максименко // Москва : Диалог-МИФИ, 2002. — 528 с.

2. Жигалов, К.А. Обеспечение безопасности облачной инфраструктуры. [Текст]: дипломная работа / К.А. Жигалов. Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ). Факультет телекоммуникаций и радиотехники (ФТР). Кафедра Мультисервисных сетей и информационной безопасности: науч. рук. А.С. Раков - Самара. 2017. - 78 с.

3. *Информационные технологии : учебник / Ю. Ю. Громов, И. В. Дидрих, О. Г. Иванова, М. А. Ивановский, В. Г. Однолько. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2015. – 260 с*

UDC 004.63

RESEARCH WORK CLOUD STORAGE SECURITY

Akbarzhonov A.B., Elmurodov Sh.Sh.

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

Asadchaya E.V. – assistant of the Department of ICSD

Annotation. This article discusses the main security threats to cloud storage, such as data leaks, malicious attacks, unauthorized access to data, etc. It also describes the main security measures that can be taken to protect cloud storage, including encryption, authentication, authorization, monitoring, and data audit.

Keywords: security, encryption, authorization.