Е. Е. Струкачева, Д. Д. Джалилзода, А. А. Захаров
Тюменский государственный университет, г. Тюмень
УДК 004.056.5

МОДЕЛЬ УГРОЗ И МЕТОДЫ ЗАЩИТЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СОЗДАННОГО ФАЙЛОХРАНИЛИЩА

Аннотация. В данной научной статье проведен обзор модели угроз для облачного файлохранилища, а также предложены методы и технологии, которые могут быть использованы для обеспечения безопасности данного компонента информационной инфраструктуры, описана классификация угроз и методов защиты.
Ключевые слова: облачное файлохранилище, модель угроз, методы защиты, анализ рисков.

Введение. В современном информационном обществе облачные хранилища становятся все более привлекательным средством управления данными и приложениями для бизнес-компаний [1]. Однако отмечается, что многие компании не готовы внедрять технологию облачных хранилищ из-за отсутствия соответствующей политики контроля безопасности и недостатков в механизмах защиты, что ведет к возникновению проблем в облачных вычислениях [2]. Таким образом, существуют две основные проблемы безопасности, которые требуется решить: защита целостности данных и контроль доступа к данным.

Для решения проблемы защиты целостности данных в облачных системах хранения данных был предложен протокол динамического аудита, обладающий возможностью поддержки динамического и пакетного аудита [3]. Для обеспечения контроля доступа к данным в облачных системах были предложены две эффективные и безопасные схемы управления доступом к данным: ABAC (Attribute-Based Access Control) для систем с одним уровнем управления и DAC-MACS (Decentralized Access Control with Multiple Authorities) для систем с несколькими полномочиями. Однако метод шифрования на основе атрибутов политики зашифрованного текста CP-ABE (Cipher-Policy Attribute-Based Encryption) не может быть применен для контроля доступа к данным в облачных системах хранения

данных из-за проблемы отзыва атрибута [3]. В связи с этим были предложены новые методы отзыва CP-ABE, которые могут быть использованы как в ABAC, так и в DAC-MACS. Одним из недостатков метода шифрования на основе атрибутов политики зашифрованного текста (CP-ABE) для контроля доступа к данным в облачных системах хранения данных является проблема отзыва атрибута, которая ограничивает возможность эффективного удаления или изменения прав доступа на основе атрибутов пользователя [3].

Для обеспечения целостности данных в облачных системах хранения, был предложен независимый механизм для обеспечения безопасного размещения данных на сервере облачного хранилища: метод безопасного хранения данных в облаке с целью предотвращения атак по сговору для модификации сервера неавторизованными пользователями [4]. Схема использует гомоморфный токен, который представляют собой шифрованные представления данных и обеспечивают распределенную проверку данных. Предложенная схема имеет ряд преимуществ: обеспечивает интеграцию проверки целостности хранения данных и идентификацию некорректно функционирующих серверов, однако сопряжена с проблемами и недостатками, связанными с вычислительной сложностью и управлением данных.

Также был представлен прототип многопользовательской системы, разработанной для обеспечения контроля доступа к наборам данных, хранящимся в ненадежной облачной среде: механизм контроля доступа к данным без вмешательства со стороны поставщика услуг [5]. Основным инструментом для контроля доступа является схема шифрования на основе атрибутов политики шифрования с динамическими атрибутами. С использованием децентрализованного реестра на основе блокчейна, система обеспечивает сохранение неизменяемого журнала всех значимых событий безопасности, таких как генерация ключа, назначение политики доступа и запросы доступа. При передаче данных через блокчейн-регистр осуществляется передача только зашифрованных текстов хэш-кодов. Некоторые недостатки прототипа системы включают ограниченность масштабируемости и возможность возникновения задержек в обработке транзакций из-за особенностей блокчейн-технологии.

Для обеспечения защиты целостности данных и контроля доступа к ним в контексте облачных вычислений требуется установка соответствующих политик конфиденциальности, целостности и доступности данных в Соглашении об уровне обслуживания (SLA) облачного поставщика услуг (CSP) [6]. Обеспечение безопасности данных является главной проблемой в этой области, ограничивающей принятие облачных решений некоторыми организациями. Для решения этой проблемы необходимо включить политики конфиденциальности, целостности и доступности данных в SLA облачного поставщика услуг (CSP)[6]. Конфиденциальная информация должна быть строго контролируема и при необходимости зашифрована. Эффективные механизмы аудита обеспечивают целостность данных и контроль их использования.

Проблема исследования. Поскольку, с одной стороны, применение облачных хранилищ не обеспечивает абсолютную безопасность данных, то определение потенциальных уязвимостей и способов их предотвращения, создав модель угроз- позволит обеспечить конфиденциальность, целостность и доступность данных собственного файлохранилища

Целью данной работы является разработка модели угроз и методов защиты для обеспечения безопасности разработанного облачного файлохранилища.

Для достижения поставленной цели необходимо решение следующих задач:

- Проанализировать потенциальные угрозы для разработанного облачного файлохранилища
- Исследовать различные аспекты и характеристики уязвимостей для облачного файлохранилища
- Оценить риски безопасности облачного файлохранилища с использованием качественного и количественного анализа рисков.
- Разработать список контрмер для защиты облачного файлохранилища от выявленных угроз.
- Провести тестирования разработанных методов защиты для обеспечения безопасности созданного облачного файлохранилища.

Материалы и методы. Файлохранилище является незаменимым инструментом для современных бизнесов, поскольку позволяет работать с файлами и документами эффективно и безопасно. Однако, в процессе работы с файлохранилищем возникают различные угрозы, которые могут негативно повлиять на безопасность и конфиденциальность данных компании.

Именно поэтому для обеспечения безопасности информационных систем необходимо создать модель угроз, которая позволит получить детальное описание всех возможных угроз, учитывая потенциальные уязвимости, определяя наиболее эффективные контрмеры для защиты информационной системы, предотвратив возможные атаки.

Основные элементы модели угроз: уязвимости, угрозы, риски и контрмеры. Уязвимости — это существующие в информационной системе недостатки, которые могут быть использованы злоумышленником для нарушения ее конфиденциальности, целостности или доступности. Угрозы — это потенциальные атаки на информационную систему, которые могут привести к утечке информации или нарушению ее целостности. Риски — это вероятность возникновения угрозы и ее последствия для информационной системы. Контрмеры — это меры по защите от угроз, которые помогают минимизировать риски и предотвращать возможные атаки.

1. Наиболее распространенные потенциальные угрозы безопасности файлохранилища:

- несанкционированный доступ: возможность несанкционированного доступа к данным в облачном хранилище через компрометацию учетных данных пользователя, слабые пароли или уязвимости в системе безопасности;
- утечка данных: возможность утечки данных из-за ошибок на стороне поставщика облачных услуг, ошибок на стороне пользователя или злонамеренных действий со стороны третьих лиц;
- вредоносные программы: возможность инфицирования облачного хранилища вредоносными программами, которые могут заразить все файлы в облачном хранилище или даже распространиться на другие устройства;

• атаки на облачного хранилища: возможность атак на облачное хранилище, такие как DDoS-атаки, фишинг, инженерия социальной инженерии или другие методы, которые могут привести к нарушению доступности и целостности данных;

• нарушение соответствия: возможность нарушения соответствия требованиям законодательства и стандартов в области безопасности данных, таких как HIPAA или PCI DSS, что может привести к существенным финансовым штрафам и утрате доверия клиентов;

• неправильная конфигурация: возможность нарушения безопасности из-за неправильной конфигурации системы, такой как открытый доступ к файлам без необходимой аутентификации и авторизации, неправильное использование шифрования или отсутствие резервного копирования данных.

2. Уязвимости облачного файлохранилища могут проявляться в различных аспектах и обладать разной характеристикой:

• недостаточная аутентификация и авторизация пользователей;
• недостаточное шифрование данных;
• недостаточная защита от вредоносных программ;
• недостаточное резервное копирование данных;
• недостаточный контроль доступа к данным;
• недостаточный контроль целостности данных;
• недостаточная защита от DDoS-атак

3. Для количественного анализа рисков в облачных хранилищах мы применили матрицу рисков, которая позволила определить вероятность возникновения каждой уязвимости и ее потенциальные последствия с использованием шкалы оценки вероятности и влияния на бизнес.

Шкала вероятности:

1. Очень низкая вероятность.
2. Низкая вероятность.
3. Средняя вероятность.
4. Высокая вероятность.
5. Очень высокая вероятность.

Шкала влияния на бизнес:

1. Незначительное влияние.
2. Умеренное влияние.
3. Значительное влияние.
4. Критическое влияние.
5. Разрушительное влияние.

После заполнения матрицы рисков для каждой уязвимости вычисляется общий риск путем умножения вероятности на последствия (табл. 1).

Таблица 1

Матрица количественного анализа рисков

Уязвимость	*Вероятность*	*Последствия*	*Риск*
Недостаточная аутентификация и авторизация пользователей	4	4	16
Недостаточное шифрование данных	3	4	12
Недостаточная защита от вредоносных программ	3	4	12
Недостаточное резервное копирование данных	2	4	8
Недостаточный контроль доступа к данным	4	4	16
Недостаточный контроль целостности данных	3	4	12
Недостаточная защита от DDoS-атак	3	4	12

Полученная таблица рисков для уязвимостей облачных хранилищ позволяет выявить наиболее критические риски и принять соответствующие меры по уменьшению вероятности и последствий их возникновения.

4. Качественный анализ рисков позволяет оценить вероятность возникновения неблагоприятных событий и их влияние на цели и задачи организации.

• *Недостаточная аутентификация и авторизация пользователей:* может привести к нежелательному доступу к данным, что может привести к утечкам конфиденциальной информации и нарушению приватности пользователей.

• *Недостаточное шифрование данных:* может привести к возможности атаки с использованием метода перебора, что может привести к компрометации конфиденциальных данных.

• *Недостаточная защита от вредоносных программ:* может привести к заражению файлов в облачном хранилище и распространению вредоносных программ на другие устройства.

• *Недостаточное резервное копирование данных:* может привести к потере данных в случае сбоя в облачном хранилище.

• *Недостаточный контроль доступа к данным:* может привести к нежелательному доступу к данным и утечке информации, что может повлечь за собой финансовые и репутационные потери.

• *Недостаточный контроль целостности данных:* может привести к возможности модификации данных злоумышленником, что может привести к искажению информации и нарушению целостности данных.

• *Недостаточная защита от DDoS-атак*: может привести к недоступности облачного хранилища для легитимных пользователей.

5. Для обеспечения безопасности облачного файлохранилища следует реализовать соответствующие контрмеры:

• использовать средства шифрования данных;

• ограничить доступ к конфиденциальной информации только авторизованным пользователям и контролировать их доступ;

• использовать средства защиты от вредоносных программ и устанавливать обновления безопасности, чтобы устранять известные уязвимости;

• использовать средства обнаружения и предотвращения атак, а также механизмы аудита безопасности;

• регулярно проверять соответствие стандартам безопасности и соблюдать политику безопасности, связанную с обработкой и хранением конфиденциальной информации;

• использовать средства автоматизации, такие как системы управления конфигурацией;

• использовать механизмы распределения нагрузки и средства обнаружения атак для защиты от DDoS-атак;

• использовать средства автоматического резервного копирования и периодически проверять их работоспособность.

Результаты. Исходя из таблицы оценки рисков, можно выделить несколько наиболее критических рисков для облачного файлохранилища:

- Недостаточная аутентификация и авторизация пользователей.
- Недостаточный контроль доступа к данным.

Обе эти уязвимости имеют высокий уровень вероятности и серьезные последствия, что делает риск значительным. Недостаточное шифрование данных, недостаточная защита от вредоносных программ, недостаточный контроль целостности данных и недостаточная защита от DDoS-атак также являются значимыми рисками, но их уровень вероятности ниже, чем у первых двух.

В контексте разработки проекта, основными объектами защиты являются вычислительные активы, так как система функционирует пока в неполном режиме, то есть находится на стадии разработки. Для обеспечения безопасности проекта была реализована защита от внешних атак через сеть Интернет, включая защиту от DDoS-атак, которая заключается в намеренном создании условий, при которых недобросовестные пользователи системы не могут получить доступ к системным ресурсам, был учтен вид атаки brute-force.

Кроме того, на стадии настройки и тестирования оборудования была обнаружена попытка несанкционированного доступа к ресурсам, в результате чего была выполнена доработка, включающая базовые настройки операционной системы, такие как групповая политика, разграничение прав доступа к ресурсам и данным пользователей, а также настройка межсетевого экрана для проброса и переадресации портов. Также была настроена система оповещения пользователя о несанкционированном доступе и настроен межсетевой экран, включая проброс и переадресацию портов. Все эти меры были реализованы для обеспечения надежной защиты вычислительных активов проекта.

Заключение. В результате проведенного исследования были выявлены наиболее распространенные угрозы и уязвимости облачного файлохранилища, а также разработаны методы защиты, которые помогут улучшить безопасность таких систем. Проведенный анализ

рисков с использованием качественного и количественного подходов позволил оценить уровень риска безопасности облачного файлохранилища и разработать соответствующие контрмеры.

Тестирование разработанных методов защиты показало их эффективность и возможность использования для обеспечения безопасности облачного файлохранилища. Таким образом, использование модели угроз и методов защиты является эффективным способом обеспечения безопасности облачных файлохранилищ.

СПИСОК ЛИТЕРАТУРЫ

1. Влияние условий эксплуатации на наработку штанговых винтовых насосных установок / Б. М. Латыпов, С. А. Дремлюга, Е. В. Чупашева [и др.]. — Текст : непосредственный // Нефтегазовое дело. — 2016. — Т. 15, № 2. — С. 55-60.
2. Джаялекшми М. Б. Исследование проблем безопасности хранения данных в облачных вычислениях / М. Б. Джаялекшми, С. Ш. Кришнавени. — Текст : непосредственный // Индийский журнал науки и техники. — 2015. — № 8. — С. 24-29.
3. Прасад Ш. С., Исследование безопасности облачного хранилища данных / Ш. С. Прасад, А. К. Ядава. — Текст : непосредственный // Международный журнал исследований в области прикладной науки и инженерных технологий. — 2022. — С. 48-56.
4. Кулкарни У. Д. Хранилище файлов в облаке с использованием криптографии / У. Д. Кулкарни, Р. Мансури, Р. Адикане. — Текст : непосредственный // Международный журнал исследований в области прикладной науки и инженерных технологий. — 2022. — С. 73-84.
5. Обеспечение безопасности хранения данных в облачных вычислениях / К. Ван, Р. Ван, К. Рен, У. Лу. — Текст : непосредственный // Международный семинар по качеству обслуживания. — США, Чикаго: ECE, 2009. — С. 78-87.
6. Суходольский И. Система контроля доступа к облачному хранилищу на основе блокчейна / И. Суходольский, С. Запечников. — Текст : непосредственный // Конференция молодых исследователей России в области электротехники и электроники IEEE. — 2018. — С. 30-38.
7. Полный обзор конфиденциальности и безопасности данных для облачного хранилища / Н. Ахтар, Б. Керим, Д. Ю. Первей, С. Правин. — Текст: непосредственный // Международный журнал научных исследований в области науки, техники и технологий. — 2021. — № 2394. — С. 113-153.