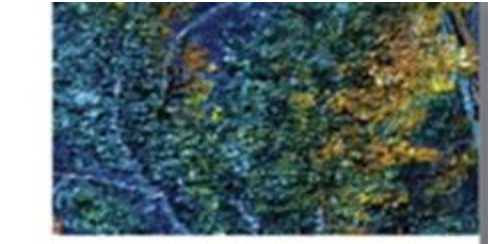

INTERNATIONAL SCIENCE REVIEWS

AIU

№1 (5) 2024

Natural Sciences and Technologies series

www.aiu.kz

ISSN: 2707-4862

ASTANA INTERNATIONAL UNIVERSITY

INTERNATIONAL SCIENCE REVIEWS
Natural Sciences and Technologies series

Has been published since 2020

№1 (5) 2024

Astana

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz

International Sciense Reviews NST - 76153
International Science Reviews
Natural Sciences and Technologies series
Owner: Astana International University
Periodicity: quarterly
Circulation: 500 copies

CONTENT

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

Садибек Е.Е, Кусепова Л.Т., Назырова А.Е.

Международный университет Астана, Астана, Казахстан
elnur.sadibek55222@mail.ru

Аннотация. Облачные сервисы являются неотъемлемой частью современных информационных технологий и предоставляют широкий спектр выгод для организаций. Однако безопасность данных в облаке остается приоритетной задачей. Эта статья обсуждает важность обеспечения безопасности данных в облачных сервисах и выделяет ключевые аспекты.

Ключевые слова: Защита данных, доступность, надежность, защита от кибератак, управление рисками, политика безопасности.

ВВЕДЕНИЕ

В современной информационной эпохе облачные сервисы стали неотъемлемой составной частью как личной, так и корпоративной деятельности. Эти службы представляют собой сетевые вычислительные ресурсы и услуги, предоставляемые через Интернет, что позволяет пользователям хранить, обрабатывать и получать доступ к данным и приложениям, размещенным на удаленных серверах. Сюда включается хостинг веб-приложений, облачное хранение данных, а также облачные вычисления, чтобы назвать только несколько аспектов (рисунок 1).

Облачные сервисы разделяются на несколько основных моделей:

IaaS (Infrastructure as a Service): Предоставление вычислительных ресурсов, сетевой инфраструктуры и хранилища данных в виде виртуальных машин, серверов и хранилища. Примерами являются Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP).

PaaS (Platform as a Service): Предоставление платформы для разработки, тестирования и развертывания приложений, освобождая от необходимости управления инфраструктурой. Примерами являются Heroku, Google App Engine и Microsoft Azure App Service.

SaaS (Software as a Service): Предоставление готовых приложений и сервисов через Интернет, с возможностью использования без необходимости установки и обслуживания. Примерами могут служить Gmail, Microsoft Office 365 и Salesforce.

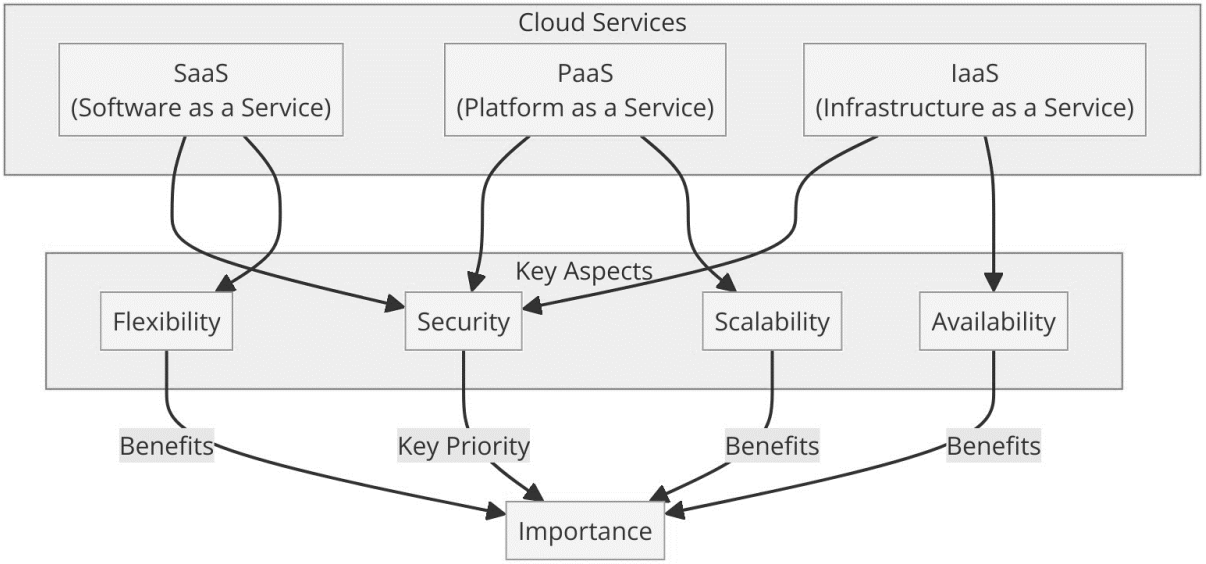

Рисунок 1 - Взаимосвязь облачных сервисов и ключевых аспектов безопасности

Актуальность облачных сервисов в наше время трудно переоценить. Они обеспечивают гибкость, масштабируемость и доступность данных и приложений в мировом масштабе. Это означает, что как организации, так и частные лица могут легко обмениваться информацией и работать с данными практически в любой точке мира, при наличии доступа в Интернете.

Рассмотрение важных аспектов безопасности в контексте облачных сервисов является неотъемлемой составляющей современной информационной инфраструктуры (рисунок 2).

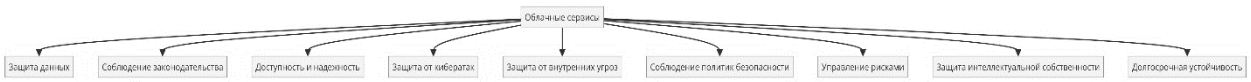

Рисунок 2 - Ключевые элементы безопасности в облачных сервисах

Защита данных, соблюдение законодательства, обеспечение доступности и надежности сервисов, защита от кибератак и внутренних угроз, соблюдение политик безопасности, управление рисками, защита интеллектуальной собственности и обеспечение долгосрочной устойчивости - ключевые аспекты, которые обеспечивают сохранность и эффективное использование облачных ресурсов. Эффективная безопасность в облачных сервисах не только защищает данные и операции, но и способствует укреплению доверия пользователей и поддержанию преимуществ, которые предоставляют эти сервисы в современной цифровой экосистеме.

Риски безопасности в облачных сервисах

Диаграмма "Риски безопасности в облачных сервисах" представляет собой ментальную карту, разбитую на три основные категории: "Утрата данных", "Последствия потери данных" и "Меры предосторожности", каждая из которых детализирует ключевые аспекты и стратегии управления рисками безопасности данных в облачных сервисах.

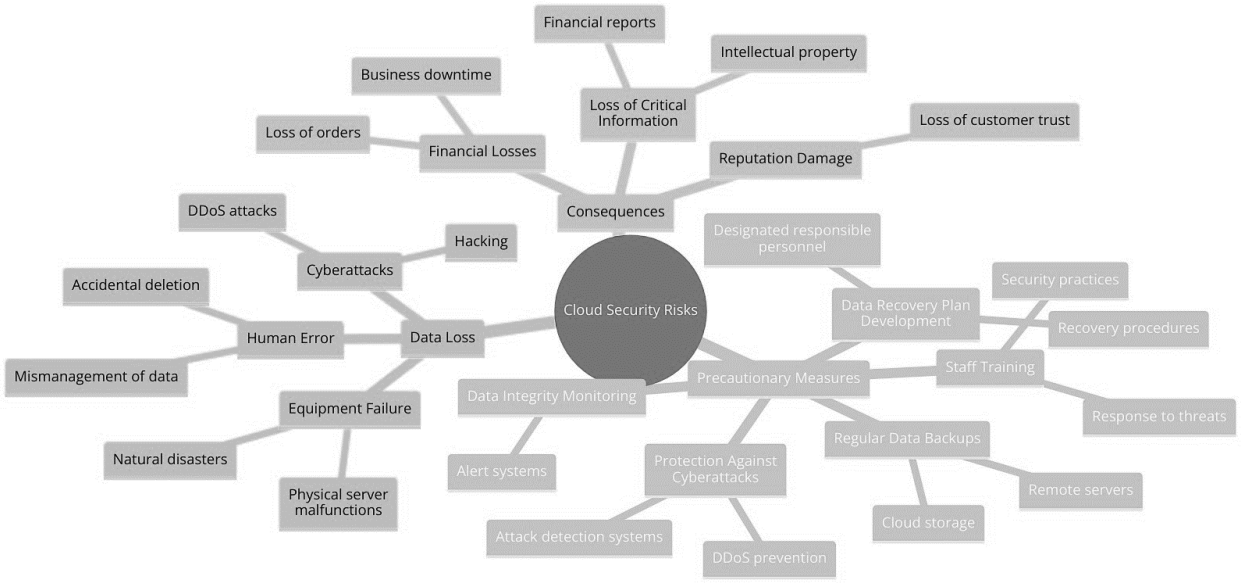

Рисунок 3 - Риски безопасности в облачных сервисах

В разделе "Утрата данных" выделены три основные причины потери данных: неисправности оборудования, включая сбои физических серверов и последствия природных катастроф; человеческие ошибки, такие как неправильное удаление файлов и некорректное управление данными; а также кибератаки, включая DDoS атаки и хакерские взломы.

"Последствия потери данных" охватывают финансовые потери из-за простоев в работе, потери заказов и клиентов; ущерб репутации, влекущий за собой потерю доверия со стороны клиентов и общественности; а также потерю критически важной информации, такой как финансовые отчеты и интеллектуальная собственность.

В секции "Меры предосторожности" представлены рекомендации по минимизации рисков потери данных: регулярное создание резервных копий данных на удаленные серверы или в облачное хранилище; мониторинг целостности данных для оперативного выявления и реагирования на проблемы; разработка и проверка плана восстановления данных, включая процедуры восстановления и назначение ответственных лиц; защита от кибератак через применение механизмов обнаружения и сдерживания атак; а также обучение персонала основам безопасности данных и методам предотвращения угроз.

Нарушение конфиденциальности данных в облачных сервисах

Диаграмма "Нарушение конфиденциальности данных в облачных сервисах" представляет собой ментальную карту, систематизирующую ключевые аспекты, связанные с рисками для секретности данных, их последствиями и мерами предосторожности для их предотвращения в контексте облачных вычислений(рисунок 4).

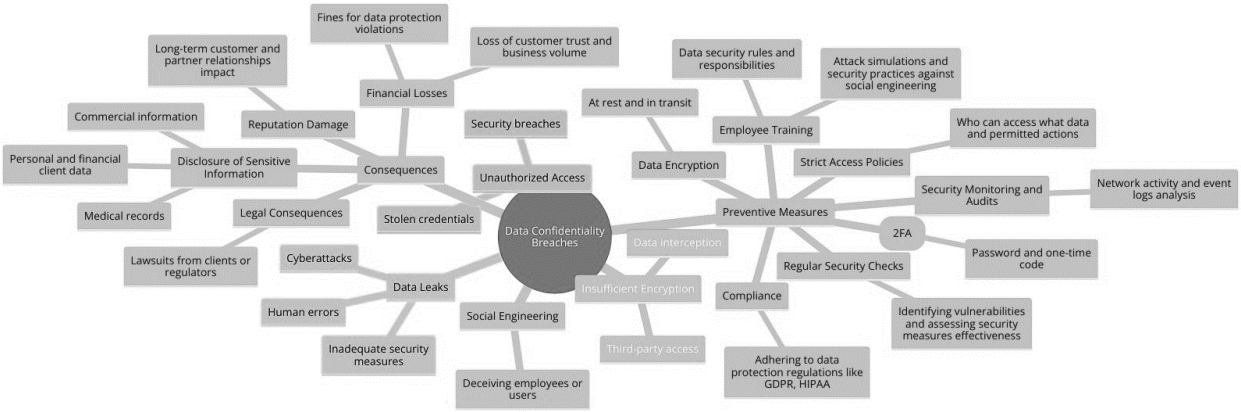

Рисунок 4 - Нарушение конфиденциальности данных в облачных сервисах

Источники рисков конфиденциальности включают неавторизованный доступ через украденные учетные данные или нарушения уровня безопасности, утечки данных, обусловленные человеческими ошибками, недостаточными мерами безопасности или кибератаками, недостаточное шифрование, подразумевающее риск перехвата и чтения данных третьими сторонами, а также социальную инженерию, направленную на обман сотрудников или пользователей для доступа к конфиденциальной информации.

Последствия нарушения конфиденциальности охватывают раскрытие чувствительной информации, включая личные и финансовые данные клиентов, медицинские записи и коммерческую информацию, что может привести к финансовым убыткам, ущербу репутации организации и юридическим последствиям, в том числе судебным искам и штрафам за нарушение законодательства о защите данных.

Меры предосторожности, направленные на предотвращение нарушения конфиденциальности данных, включают шифрование данных в состоянии покоя и при передаче, внедрение двухфакторной аутентификации для добавления дополнительного уровня безопасности при входе в систему, разработку строгих правил доступа, регулярный мониторинг и аудит безопасности для выявления подозрительной активности, обучение сотрудников правилам безопасности данных, проведение регулярных проверок безопасности для идентификации уязвимостей и оценки эффективности мер безопасности, а также соблюдение

нормативных требований и законодательства о защите данных, таких как GDPR и HIPAA.

Киберугрозы для облачных сервисов

Диаграмма "Киберугрозы для облачных сервисов" представляет собой структурированное визуальное изображение, категоризирующее различные типы кибератак, их потенциальные последствия для облачных сервисов, а также рекомендуемые меры предосторожности для предотвращения и смягчения угроз(рисунок 5). Основные категории включают атаки на доступность, такие как DDoS, направленные на перегрузку серверов и нарушение работы сервисов; перехват данных, целью которого является кража чувствительной информации; взлом учетных записей для несанкционированного доступа к данным и ресурсам; вредоносное программное обеспечение для повреждения данных и инфраструктуры; и фишинговые атаки для обмана сотрудников и получения конфиденциальных данных.

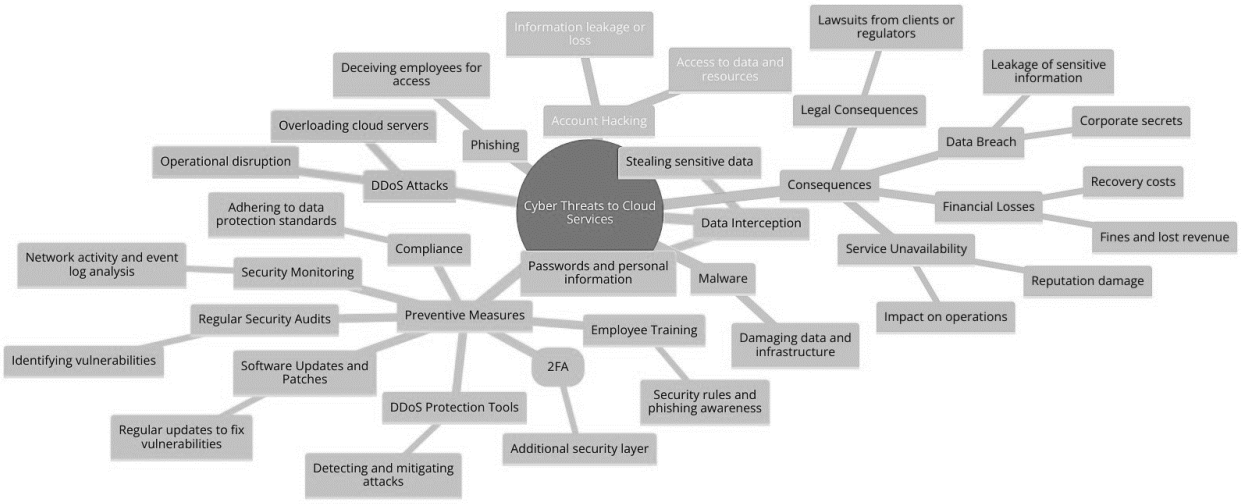

Рисунок 5 - Киберугрозы для облачных сервисов

Последствия этих угроз могут включать недоступность сервисов, утечку данных, финансовые убытки, а также юридические последствия в случае нарушения законодательства о защите данных. Для защиты облачных сервисов рекомендуется использовать инструменты защиты от DDoS-атак, двухфакторную аутентификацию, регулярные обновления и патчи программного обеспечения, обучение персонала по безопасности, мониторинг безопасности и проведение регулярных аудитов безопасности, а также соблюдение стандартов и нормативов по защите данных.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности в рамках облачных сервисов представляет собой сложную и критически значимую задачу в современной эпохе, когда множество

компаний воспользуется облачным хранилищем и обработкой данных. Эта проблема охватывает как аспекты защиты данных, так и широкие меры информационной безопасности. В данной статье мы тщательно исследовали ключевые аспекты обеспечения безопасности в сфере облачных сервисов и представили советы о наилучших методах для достижения данной цели.

Мы выявили, что угрозы безопасности в сфере облачных сервисов включают в себя опасность потери данных, утечку конфиденциальной информации и возможные кибератаки. Потеря данных может возникнуть по различным причинам, таким как технические сбои, программные ошибки и человеческие недоразумения, поэтому регулярное создание резервных копий данных становится обязательной мерой безопасности. Утечка конфиденциальной информации может быть следствием несанкционированного доступа к данным, но использование шифрования и строгого контроля доступа способствует предотвращению таких инцидентов. Кибератаки могут иметь серьезные последствия, и меры мониторинга безопасности, регулярное обновление программного обеспечения и использование безопасных систем помогают уменьшить этот риск.

Средства обеспечения безопасности включают разработку политики безопасности, шифрование данных, процедуры идентификации и аутентификации пользователей, регулярное обновление и контроль состояния систем, создание резервных копий данных, обеспечение физической безопасности, контроль и управление угрозами, а также соблюдение требований и нормативов, таких как GDPR и HIPAA. Соблюдение законодательных и нормативных требований помогает не только защитить данные, но и предотвратить возможные юридические последствия.

Внедрение наилучших практик в сфере обеспечения безопасности облачных сервисов включает разработку политики безопасности, использование шифрования данных, проверку личности и аутентификацию пользователей, регулярное обновление и наблюдение за системами, создание резервных копий данных, обеспечение физической безопасности, контроль и управление угрозами, а также соблюдение требований и нормативов. Постоянное усовершенствование стратегии безопасности также играет ключевую роль. Гарантирование безопасности облачных сервисов требует всестороннего и системного подхода. Организации должны вкладывать ресурсы в область безопасности, обучать свой персонал и регулярно обновлять свои меры безопасности, чтобы адаптироваться к новым угрозам и обеспечивать надежность и конфиденциальность данных в сфере облачных сервисов.

СПИСКИ ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Haider Al-Khateeb. "A Survey of Cloud Computing Security Management"

2. Jinshu Su, Jinshu Su, and Han Zhao. "Security and Privacy Issues in Cloud Computing: A Survey"
3. Prashant K. Jadhav, Poonam S. Patil, and Sunil B. Manke."Data Security in Cloud Computing: A Comprehensive Survey"
4. Arati Baliga, K. R. Anjali "Security Issues in Cloud Environments: A Survey"
5. Krishna Kant "Cloud Computing Security Challenges and Solutions: A Survey"