УДК 004

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Секлетова Н. Н., к.п.н.
доцент кафедры ИСТ
Тучкова А. С.
ст. преподаватель кафедры ИСТ
Салихов Р. Р.
Студент
Субханкулов А. М.
Студент
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»
Российская Федерация, г. Самара

Аннотация. В статье исследуются проблемы и вызовы, с которыми организации сталкиваются при использовании облачных технологий для управления документооборотом. Предлагаются решения для обеспечения информационной безопасности в таких средах. Рассматриваются преимущества облачных технологий, актуальные проблемы информационной безопасности и меры по их решению.

Ключевые слова: облачные технологии, документооборот, информационная безопасность.

ENSURING INFORMATION SECURITY WHEN AUTOMATING DOCUMENT FLOW USING CLOUD TECHNOLOGIES

Sekletova N. N., Candidate of Pedagogical Sciences.
Associate Professor of the IST Department
Tuchkova A. S.
senior lecturer of the IST department
Salikhov R. R.
Student
Subkhankulov A. M.
Student
Povolzhskiy State University of Telecommunications and Informatics
Russian Federation, Samara, Russia

Abstract. The article explores the challenges organizations face when using cloud technologies for document management. Solutions for ensuring information security in such environments are proposed. The advantages of cloud technologies, current information security issues, and measures to address them are discussed.

Keywords: cloud technologies, document management, information security.

Современный мир бизнеса стал неотъемлемым участником цифровой революции, преобразуя свои процессы и стратегии под влиянием технологических инноваций. Одним из ключевых направлений этой трансформации является автоматизация документооборота с использованием облачных технологий. Облачные решения позволяют организациям эффективно управлять документами, обеспечивая доступность и мобильность сотрудников, сокращая издержки на инфраструктуру и ускоряя процессы работы.

Однако, вместе с преимуществами, которые предоставляют облачные технологии, возникают и новые вызовы в области информационной безопасности. Целью данной статьи является рассмотрение вопросов

обеспечения информационной безопасности при автоматизации документооборота с применением облачных технологий.

Облачные технологии представляют собой способ предоставления вычислительных ресурсов, таких как хранилища данных, вычислительная мощность и приложения, через интернет [1]. Они основаны на модели предоставления услуг (как правило, через Интернет), при которой пользователи получают доступ к облачным ресурсам по запросу, без необходимости владеть и управлять физическим оборудованием или программным обеспечением.

Использование облачных технологий в документообороте предоставляет множество преимуществ для современных организаций. Основные из них рассмотрены ниже:

1. Доступность и мобильность: облачные решения позволяют сотрудникам работать с документами из любой точки мира при наличии интернет-соединения. Это повышает мобильность и гибкость рабочих процессов.

2. Сокращение затрат: организации могут сэкономить средства, которые ранее требовались на закупку и обслуживание собственной инфраструктуры для хранения данных и обработки документов.

3. Масштабируемость: облачные ресурсы могут быть масштабированы по мере роста бизнеса. Организации могут легко увеличивать или уменьшать объем хранимых данных и вычислительных мощностей в зависимости от потребностей.

4. Автоматизация и оптимизация процессов: облачные сервисы предоставляют инструменты для автоматизации многих процессов документооборота, таких как согласование, уведомления и контроль версий. Это позволяет повысить эффективность и скорость выполнения задач.

5. Более низкие риски потери данных: облачные провайдеры обычно обеспечивают резервное копирование данных и защиту от сбоев, что

уменьшает риск потери информации по сравнению с локальными хранилищами.

Активное использование облачных сервисов и хранилищ данных ставит перед организациями задачу обеспечения безопасности конфиденциальной информации, защиты от киберугроз и предотвращения утечек данных. В ходе исследования были выявлены факторы уязвимости облачных сервисов. До 85% взломов облачных сервисов — это проблема администрирования. До 30% всех взломов производятся с украденными данными учѐтных записей пользователей [3].

При использовании облачных технологий существует несколько типов атак, к которым организации должны быть готовы:

1. Атаки на учётные записи: злоумышленники могут пытаться получить доступ к учетным записям пользователей облачных сервисов с целью кражи конфиденциальной информации или нарушения работоспособности систем.

2. Межсерверные атаки: атаки, направленные на серверы облачных провайдеров, могут привести к нарушению работы сервисов и утечке данных.

3. Атаки на протоколы и шифрование: нарушение протоколов безопасности или слабые методы шифрования могут стать объектом атак, в результате чего данные могут быть скомпрометированы.

Встроенные механизмы безопасности в облачных сервисах представляют собой основу защиты данных в облачном документообороте. Однако, для обеспечения полной безопасности необходимо применять дополнительные меры защиты. Рассмотрим основные меры по обеспечению информационной безопасности в облачном документообороте:

1. Шифрование данных. Шифрование данных является одним из наиболее эффективных и надежных способов защиты конфиденциальной информации. При использовании облачных сервисов следует обеспечить шифрование данных при хранении и передачи. Это обеспечит защиту от

несанкционированного доступа к данным в случае утечки или перехвата трафика, так как шифрование защищает саму информацию, а не доступ к ней.

2. Управление доступом. Контроль доступа к данным в облачных системах играет ключевую роль в обеспечении безопасности. Организации должны строго регулировать доступ к документам, определяя права доступа для каждого пользователя или группы пользователей.

3. Многоуровневая аутентификация. Внедрение многоуровневой аутентификации добавляет дополнительный слой защиты для учетных записей пользователей. Кроме стандартного пароля, пользователю может потребоваться подтверждение своей личности через дополнительный фактор, такой как SMS-код, биометрические данные или аппаратный токен.

4. Мониторинг и анализ безопасности. Внедрение систем мониторинга и анализа безопасности позволяет обнаруживать аномальное поведение пользователей и потенциальные угрозы безопасности.

Применение этих мер по обеспечению информационной безопасности в облачном документообороте поможет организациям минимизировать риски и защитить конфиденциальность своих данных.

В целом, облачные технологии продолжат играть ключевую роль в развитии современных организаций, и обеспечение безопасности информации в облачном документообороте останется одним из важнейших приоритетов для успешной деятельности бизнеса в цифровой эпохе.

Список источников

1. Дж. Чен и Л. Чжоу Эмпирическое исследование облачной системы управления документами: NetDocuments, Journal of Computer Information Systems, том 60, № 6, стр. 530-539, 2020.

2. Назиев, М. И. Сущность и проблемы обеспечения информационной безопасности системы электронного документооборота в современной организации / М. И. Назиев, Л. Р. Магомаева // Наука и творчество: вклад молодежи : Сборник материалов IV всероссийской молодежной научно-практической конференции студентов, аспирантов и

молодых ученых, Махачкала, 08–09 ноября 2023 года. – Махачкала: Типография ФОРМАТ, 2023. – С. 40-44. – EDN KXRIMU.

3. Проблемы безопасности при использовании облачных технологий для автоматизации организаций. [Электронный ресурс] Tadviser.ru. Режим доступа: URL: https://www.tadviser.ru/