Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

# ОБЛАЧНЫЕ ТЕХНОЛОГИИ РАБОТЫ С ДОКУМЕНТАМИ

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Экономика и управление»
профилизации «Управление документами в организации»

Идентификационный код ВКР: 328

Екатеринбург, 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт гуманитарного и социально-экономического образования
Кафедра документоведения, истории и правового обеспечения

К ЗАЩИТЕ ДОПУСКАЮ:
И.о. заведующего кафедрой ДПО
_____И.В. Осипова
«___» _____ 20___г.

# ОБЛАЧНЫЕ ТЕХНОЛОГИИ РАБОТЫ С ДОКУМЕНТАМИ

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Экономика и управление»
профилизации «Управление документами в организации»

Идентификационный код ВКР: 328

Исполнитель:
студент группы УД-402п Т.А. Лебедева

Руководитель:
доцент кафедры ДПО,
канд. ист. наук М.Б. Ларионова

Нормоконтролер:
старший преподаватель
кафедры ДПО А.Е. Новосёлова

Екатеринбург, 2019

СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

В настоящее время методы работы с электронными документами приобретают все большую актуальность в связи с внедрением информационно-компьютерных технологий в документооборот организации.

В связи с переходом на электронный документооборот возникли два очень важных вопроса, касающихся аспектов хранения и обработки электронных документов – это поиск оптимальной технологии, предоставляющей разнообразный функционал по работе с документами, а также выбор надежного, защищенного носителя информации, обеспечивающего её долговременное хранение.

В данный момент существует несколько методов работы с электронными документами в зависимости от технологии хранения:

– внешние носители;

– локальный сервер или локальный компьютер в организации;

– программа электронного архива;

– облачная система.

Именно последнему методу – облачной технологии работы с электронными документами будет посвящена моя работа, поскольку данная технология является одной из самых современных и перспективных.

Мировая практика демонстрирует, что все больше зарубежных архивов переходит на хранение электронных документов с применением облачных систем. Облачное хранение документов – аспект, вызывающий одновременно опасения и любопытство среди будущих пользователей.

В данный момент многие компании ценят возможность хранения данных таким способом для более удобного управления, разгрузки собственной системы документооборота и потенциальной экономии средств по обслуживанию внутриорганизационной инфраструктуры. Однако существует ряд факторов, останавливающий потенциального клиента от использования «облака», в первую

очередь, вопрос безопасности данных, которые хранятся вне организации и добросовестности поставщика облачных услуг.

Для обеспечения информационной безопасности в облачных вычислениях используется множество различных современных методов защиты, в которых необходимо ориентироваться. В этом аспекте еще много проблем, в которых предстоит разобраться.

Выбор облачных технологий для работы с документами актуален в связи с тем, что он предполагает принципиально иной механизм доступа к электронным документам, значительно отличающийся от иных механизмов.

Электронные документы могут сдаваться на государственное хранение по электронным каналам связи, доступ к данным документам может осуществляться через электронный виртуальный читальный зал в сети Интернет, что позволит любому пользователю в любом субъекте Российской Федерации легко получить доступ к необходимым ему электронным документам, где бы они физически не находились[1].

Актуальность работы обусловлена необходимостью разбираться и ориентироваться современном методе работы с электронными документами – облачных технологиях.

Объект исследования – электронные документы как документированная информация в электронной форме, созданная с помощью электронно-вычислительных машин для обработки в информационных системах.

Предмет исследования – облачные технологии как современный метод работы с электронными документами

Цель работы – выявить достоинства и риски использования облачных технологий работы с электронными документами.

Для достижения поставленной цели определены следующие задачи работы:

---

[1] Александров К.С. Счет на петабайты // Машины и механизмы. 2013. № 6. С. 20.

1. Рассмотреть преимущества использования облачных систем хранения электронных документов.

2. Выявить недостатки использования облачных систем хранения электронных документов.

3. Рассмотреть проблемы защиты данных в облачных технологиях работы с электронными документами.

4. Изучить методы защиты данных в облачных технологиях работы с электронными документами.

5. Рассмотреть методы защиты данных в облачной системе электронного документооборота DirectumRX.

При написании выпускной квалификационной работы была исследована различная литература. Значительную роль для меня сыграли такие авторы как Р.К. Читчян[1], которая рассмотрела оптимизацию документооборота на предприятии при помощи облачных технологий, С.А. Овчинников[2], в научной статье которого, облачные технологии рассматриваются как фактор политического риска для электронного государственного управления, а также И.А. Котяшичев[3], в работе которого описаны проблемы защиты информации в облачных технологиях.

Такие авторы как Е.А. Широкова[4], Ф.А. Мурзин[5], Т.В. Батура, Д.Ф. Семич в своих научных трудах помогли сформировать понятие облачных технологий, а также их значение в хранении электронных документов.

---

[1] Читчян Р. К. Оптимизация документооборота на предприятии при помощи облачных технологий и перспективы их развития // Научно-исследовательские публикации. 2016. № 2. С. 26-36.

[2] Овчинников С.А. Облачные технологии как фактор политического риска электронного государственного управления // Автоматика. Вычислительная техника. 2012. № 4. С. 186-190.

[3] Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. № 6. С. 30-34.

[4] Широкова Е. А. Облачные технологии // Современные тенденции технических наук. 2011. № 14. С. 30-33.

[5] Мурзин Ф.А., Батура Т.В., Семич Д.Ф. Облачные технологии: основные понятия, задачи и тенденции развития // Программные продукты, системы и алгоритмы. 2014. № 1. С. 2-22.

В.А. Догваль[1] и А.С. Хажиева[2] в своих научных статьях рассмотрели вопросы безопасности информации в облаке.

Многие из этих авторов, отмечают, что облачные вычисления в аспекте хранения документов представляют в данный момент большой интерес как для больших корпораций, так и для мелких предприятий, для сфер науки, образования и государственного сектора.

Цель и задачи выпускной квалификационной работы обусловили выбор её структуры. Работа состоит из введения, трех глав, заключения, списка использованных источников и литературы.

[1] Догваль. Е.М. Методы повышения безопасности в сфере «облачных» технологий // Вестник АГУ. 2014. №4. С. 170-174.

[2] Хажиева А.С. Принципы защиты информации в облаке // Информационная безопасность. 2016. № 9. С. 7-15.

# 1. ОБЛАЧНЫЕ СИСТЕМЫ ХРАНЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

## 1.1. Понятие облачных технологий

С ростом использования облачных вычислений, а также программного обеспечения как услуги (SaaS) облачное хранилище стало центром внимания в вопросах хранения информации.

Локальные данные пользователя могут храниться в онлайн-пространствах, и предоставляться поставщиком в виде услуги. То есть, пользователь может не создавать свои собственные центры обработки данных, а вместо этого, подать заявку на заказ услуг от поставщика. Таким образом можно сэкономить на дорогостоящей аппаратной и программной инфраструктуре.

По результатам исследования компании DC Russia Cloud Services Market, российского рынка облачных услуг, в 2017 году его объем составил порядка 663 миллионов долларов, что на 49% больше, чем в прошлом. По прогнозам аналитиков, к 2022 году его объем может составить порядка 1,5 миллиарда долларов. В исследовании принимали участие российские и международные провайдеры облачных услуг и использовались такие методы как интервью, анализ опубликованных пресс-релизов и публичные финансовые отчеты[1].

Идея того, что сейчас мы называем облачными вычислениями, впервые была озвучена Джозефом Ликлайдером в 1970 году, когда он был ответственным за разработку ARPANET (Advanced Research Projects Agency Network)[2].

Идея Джозефа Линклайдера заключалась в том, чтобы каждый человек, подключенный к сети мог получать не только данные, но и программы.

---

[1] Мурзин Ф. А., Батура Т. В., Семич Д. Ф. Облачные технологии: основные понятия, задачи и тенденции развития // Программные продукты, системы и алгоритмы. 2014. № 1. С. 2.

[2] Широкова Е. А. Облачные технологии // Современные тенденции технических наук. 2011. № 14. С. 31.

Другой ученый - Джон Маккарти, говорил о том, что вычислительные мощности будут предоставляться пользователям в виде услуги. На этом этапе развитие облачных технологий было приостановлено до 90-х годов[1].

Следующим толчком стало стремительное развитие Интернета. Его ускорение вывело эту технологию на новый уровень.

В 1999 году появилась компания Salesforce.com, которая предоставила доступ к своему приложению через сайт. Эта компания стала первой компанией, предоставившей свое программное обеспечение по принципу «программное обеспечение как сервис» (SaaS).

В 2002 году Amazon запустила свой облачный сервис, где пользователи могли хранить информацию и проводить необходимые вычисления.

В 2006 году Amazon запустила сервис Elastic Compute cloud (EC2), где пользователи могли запускать свои собственные приложения. В том же году Amazon был создан сервис AWS S3, получивший широкое признание в качестве поставщика хранилища для популярных сервисов, таких как SmugMug, Dropbox и Pinterest[2].

Таким образом, сервисы Amazon EC2 и Amazon S3 стали первыми сервисами облачных вычислений.

В настоящее время рынок облачных технологий растет, поскольку множество предприятий выбирают их с целью оптимизации своего документооборота.

Облака также получили распространение и в государственном секторе РФ. Облачные сервисы активно используют в министерствах, департаментах, федеральных службах РФ. В основном они отдают предпочтение частной модели облаков, а также отечественным службам.

---

[1] Широкова Е.А. Облачные технологии // Современные тенденции технических наук. 2011. № 14. С. 31.

[2] Там же. С. 31.

По данным опроса «РазвитиеБизнеса.Ру» 2014 г. российские компании отдают предпочтение таким облачным системам как «СКБ Контур», «Манго Телеком», «Барс Груп» и др[1]. Данные опроса представлены на рис.1.


Рисунок 1 – Соотношение поставщиков облачных услуг России[2]

Итак, рассмотрим определение облачных технологий.

Сам термин «Облако» выступает как метафора для изображения сети Интернета. Используя этот термин, разработчики старались объяснить пользователям и инвесторам, что хранение, вычисление и обработка данных происходит на их персональном компьютере, в их доме, а где-то очень далеко в «облаках», на сервере, т.е. в чужом центре обработки данных, который может находится практически в любой точке мира.

На данный момент широко распространено определение облачных технологий, которое было предложено Национальным институтом стандартов и технологий США: «Облачные технологий, представляют собой модель для обеспечения по требованию удобного сетевого доступа к общему пулу

[1] Сударкина Е.С. Облачные технологии в госсекторе: преимущества и проблемы внедрения // Электронный вестник Ростовского социально-экономического института. 2015. № 4. С.23.

[2] Там же. С. 24.

настраиваемых вычислительных ресурсов (например, сетей, серверов, систем хранения данных, приложений и услуг), которые можно быстро выделить и предоставить с минимальными управленческими усилиями или минимальным вмешательством со стороны поставщика услуг»[1].

Таким образом, облачные технологии – это технологии обработки данных, в которых компьютерные ресурсы (сервера, хранилища, базы данных, сетевое оборудование, программное обеспечение и т. д.) предоставляются Интернет-пользователю как онлайн-сервис.

Для наглядности на рис.2 приведена иллюстрация, в которой отражено понятие облачной технологии.

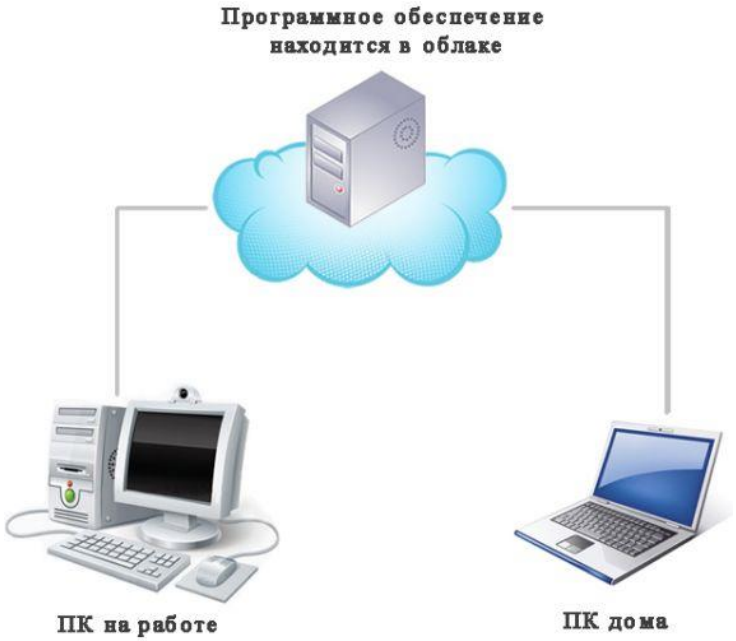


Рисунок 2 – Изображение облачной технологии[2]

Компании, которые предоставляют облачные услуги, называются поставщиками или провайдерами. Обычно они берут плату за свой сервис подобно тому, как мы платим за свет, электричество или воду. Как правило оплата производится ежемесячно. Также существуют облачные сервисы,

[1] Mell P., Grance T. The NIST Definition of Cloud Computing (Draft) // Recommendations of the National Institute of Standards and Technology. 2011. № 21. P. 146.

[2] Мурзин Ф. А., Батура Т. В., Семич Д. Ф. Облачные технологии: основные понятия, задачи и тенденции развития // Программные продукты, системы и алгоритмы. 2014. № 1. С. 3.

которые предоставляют некоторый бесплатный лимит, к ним можно отнести многие облачные файловые хранилища, например, Google Drive, Яндекс. Диск, DropBox и т.д.

Обозначим признаки облачных технологий.

Национальным институтом стандартов и технологий США зафиксированы следующие обязательные характеристики облачных вычислений[1]:

1. Самообслуживание по требованию. Потребитель в праве сам выбирать и изменять особенности предоставляемых ему услуг.

2. Универсальный доступ по сети. Потребителю доступны все услуги, не зависимо от устройства, которое он использует.

3. Объединение ресурсов. Провайдер услуг объединяет ресурсы для обслуживания множества клиентов в единое программное оборудование в условиях постоянного изменения спроса на мощности; при этом клиент контролирует только основные параметры услуги (объём данных, скорость доступа и т.д.), но фактическое распределение ресурсов выполняет поставщик.

4. Эластичность. То есть, услуги могут быть предоставлены или изменены любое время, в основном, автоматически.

5. Учёт потребления. Измеримость предоставляемых провайдером услуг, мониторинг ресурсов.

Рассмотрим виды услуг, которые предоставляют «облака» в настоящее время, их также называют моделями обслуживания.

Программное обеспечение как услуга (SaaS) – представляет собой наиболее часто используемый вариант для предприятий на облачном рынке. Провайдер предоставляет программное обеспечение, доступное пользователю через Интернет, клиент платит только за использование программного обеспечения. Большинство приложений SaaS запускаются непосредственно

[1] Mell P., Grance T. Mell P., Grance T. The NIST Definition of Cloud Computing (Draft) // Recommendations of the National Institute of Standards and Technology. 2011. № 21. P. 146.

через веб-браузер и не требуют каких-либо загрузок или установок со стороны клиента.

SaaS предоставляет многочисленные преимущества сотрудникам и компаниям, значительно сокращая время и деньги, затрачиваемые на утомительные задачи, такие как установка, управление и обновление программного обеспечения.

Примерами SaaS являются Gmail, Google Docs, Photoshop.com, Acrobat.com, Intuit QuickBooks Online, IBM LotusLive, Unyte, Salesforce.com, Sugar CRM и WebEx и т.д.

Платформа как услуга (PaaS) – это удобная платформа, позволяющая создавать специализированные приложения. Провайдер услуг предоставляет доступ к облачной среде, в которой клиенты могут создавать и использовать приложения. При этом управление операционной системой находится в руках провайдера.

В качестве примера можно привести AWS Elastic Beanstalk, Heroku, Windows Azure, Windows Azure, Boomi, Cast Iron, Google App Engine и другие.

Инфраструктура как услуга (IaaS) – пользователю предоставляется инфраструктура облачных вычислений (серверы, сеть, операционные системы и хранилище), которую он настраивает самостоятельно, в зависимости от своих нужд. IaaS позволяет предприятиям приобретать ресурсы по требованию и по мере необходимости, вместо того чтобы покупать оборудование напрямую. Клиент при этом получает полный контроль над всей инфраструктурой без необходимости ее физического обслуживания.

В пример можно привести Amazon Web Services, Linode, Rackspace, Google Cloud Storage, Parallels Cloud Server и другие.

Стоит отметить, что выше перечислены только традиционные модели облаков. В настоящее время их существует целое множество, например, BPaaS (услуги по решению бизнес-задач), DaaS (виртуальный рабочий стол), SecaaS (информационная безопасность в аренду), BaaS (резервное копирование как

сервис), DRaaS (решения по обеспечению катастрофоустойчивости), CCaaS (виртуальный контакт-центр).

В целом, каждая из этих моделей предлагает свои специфические особенности и функциональные возможности, выбор оптимальной должен исходить из цели предприятия.

Теперь давайте рассмотрим модели развертывания облачных технологий.

Итак, по модели развертывания облака разделяют на общедоступные (публичные), частные и гибридные[1].

Публичные облака – это именно то, что большинство людей называют «облаком», т.е. ИТ-услуги предоставляются клиенту через Интернет. Публичное облако называют общедоступным, потому что оно размещается у поставщика услуг (например, Amazon, Google, IBM или Microsoft). Клиенты могут пользоваться услугами, не имея возможности при этом управлять «облаком», потому что за разработку, установку, управление и обслуживание пула вычислительных ресурсов отвечает поставщик. То есть, данные могут храниться на одном физическом сервере с данными других организаций, при этом не имея доступа к данным друг друга.

Публичное облако имеет несколько преимуществ. Кроме того, что услуги предоставляются через Интернет и клиенты платят только за ресурсы, которые они используют (например, как за коммунальные услуги), организациям также можно не беспокоиться об установке и обслуживании программного обеспечения. Такое решение подойдет организации, которой необходимы определенные приложения и сервисы для выполнения своих ИТ и бизнес-операций.

Главный недостаток публичного облака относится к безопасности. Общедоступные облака часто не соответствуют нормативным требованиям безопасности, поскольку сервера находятся в разных странах, в которых правила

[1] Мурзин Ф. А., Батура Т. В., Семич Д. Ф. Облачные технологии: основные понятия, задачи и тенденции развития // Программные продукты, системы и алгоритмы. 2014. № 1. С. 8.

безопасности могут отличаться. Кроме того, проблемы с сетью могут возникнуть во время сбоев в онлайн-трафике. И, хотя модель общедоступного облака, как правило, является экономически эффективной (предполагая цены и оплату по мере использования), при перемещении больших объемов данных, расходы могут возрастать.

В пример можно привести такие онлайн-сервисы как Amazon EC2 и Amazon Simple Storage Service (S3), Salesforce.com, Google Apps/Docs, Microsoft Office Web.

Частные облака – это облачное решение, предназначенное для использования одной организацией. Пользоваться таким сервисом могут сразу несколько потребителей, например, бизнес-единицы одной организации. Ресурсы центра обработки данных могут быть расположены либо в управлении самой организации, либо управляться сторонним поставщиком за пределами территории. Вычислительные ресурсы изолированы друг от друга, доставляются через защищенную частную сеть и не передаются другим клиентам. Частное облако настраивается в соответствии с уникальными потребностями организации. Благодаря большой прозрачности и контролю над инфраструктурой организации, система работает без ущерба для безопасности и производительности. Раньше такое было возможно только с помощью выделенных локальных центров обработки данных.

Частные облака имеют такие же преимущества, как и публичные, отличие только в том, что предприятие самостоятельно занимается установкой и обеспечением облака. Частные облака стоит использовать при работе с ценной информацией, которую нельзя доверить публичному облаку. Такие облака однозначно подходят для крупных предприятий, правительственных учреждений и тех организаций, которым требуется строгий контроль за безопасностью своих данных.

Недостаток их использования – сложность создания внутреннего облака, а также высокие расходы на его разработку и использование, в разы превышающие расходы на публичные облака.

Гибридное облако – представляет собой сочетание публичных и частных облачных решений. Ресурсы обычно организованы в интегрированную инфраструктуру, где часть услуг ложится на публичное облако, а часть – к частному, т.е. управление таким облаком распределяется между предприятием и поставщиком публичного облака. Например, потребитель может хранить данные в частном облаке, а приложение – в публичном.

Преимущество данной модели в её экономически эффективности, поскольку компании могут использовать более дорогие облачные ресурсы только по мере необходимости.

Её недостаток – в трудности поддержки такой многоуровневой системы. В интеграции гибридного облаке могут быть сложности, поскольку оно представляет собой комбинацию различных облаков, данных и приложений. При разработке гибридного облака могут возникнуть серьезные проблемы совместимости во всей инфраструктуре.

В соответствии с данными опроса IDG Connect, проделанного согласно заказу Oracle, частные облака раскручены только в 32% компаний, в то время как по гибридной модели работают 36% фирм, публичные используют 17% компаний[1]. Данные опроса приведены на рис.3.


Рисунок 3 – Облачная инфраструктура в корпоративном сегменте[2]

[1] Читчян Р. К. Оптимизация документооборота на предприятии при помощи облачных технологий и перспективы их развития // Научно-исследовательские публикации. 2016. № 2. С. 6.

[2] Там же. 2016. № 2. С. 6.

В последние несколько лет в сегменте крупнейших предприятий произошел сдвиг от частных облаков в сторону гибридных моделей, когда часть ИТ потребляется из собственных дата-центров, а часть берется в аренду у внешних сервис-провайдеров[1].

Следует отметить, что такие авторы Д.В. Денисов, а также С.А. Овчинников в своих трудах, посвященных использованию облачных технологий в документообороте, среди трех вышеперечисленных моделей развертывания облаков наиболее актуальной для бизнеса в настоящее время считают частные облака.

Таким образом, мы дали понятие облачных технологий, а также рассмотрели и описали модели развертывания и модели обслуживания облачных технологий. Исходя из вышесказанного, можно сделать вывод, что самым оптимальным решением из трех моделей развертывания в организации в хранении электронных документов на данный момент являются частные облака, благодаря их высокой защищенности данных, по сравнению с остальными, а из моделей обслуживания – программное обеспечение как услуга (SaaS), благодаря её удобству, быстроте внедрения и цене. Стоит отметить, что многие облачные системы электронного документооборота используют именно эту модель.

## 1.2. Преимущества использования облачных систем хранения электронных документов

По мнению одного из «отцов» Интернета, Винта Сёрфа, который сейчас является вице-президентом Google, в недалеком будущем многие данные и документы буду утеряны вследствие устарения носителей информации[2].

---

[1] Читчян Р. К. Оптимизация документооборота на предприятии при помощи облачных технологий и перспективы их развития // Научно-исследовательские публикации. 2016. № 2. С. 7.

[2] Растамханова С. Н., Фазлетдинова А. Р., Хафизова Р. Р. «Облачное хранилище данных» в документоведческом аспекте // Молодой ученый. 2016. № 26. С. 81.

Действительно, на сегодняшний день не просто найти устройство для чтения дискет, в ближайшее время тоже самое произойдет и с дисками. В то же время устаревают форматы – разработчики ПО нередко отказываются поддерживать старые версии файлов, поэтому работать с такими версиями становиться проблемой. По возможности рекомендуется не затягивать с переводом данных с надлежащие формы.

Одна из новейших форм хранения электронных документов – облачное хранение. В настоящее время эта распространенная технология активно развивается и модифицируется на рынке систем электронного документооборота (СЭД). В настоящее время этот метод хранения популярен, особенно для малых и средних организаций в сфере бизнеса. Удаленное хранение документов по сравнению с локальным предоставляет преимущества как потребителям, так и предприятиям.

Российский рынок облачных сервисов - один из немногих секторов ИТ-рынка, который даже в условиях кризиса продолжает переживать бурный рост[1].

Облачные СЭД появились в мире совсем недавно – в 2008 году. Активно использоваться в нашей стране они стали примерно с 2012 года. В основном распространены публичные облака, но государственные структуры в основном используют частные и это относится не только к России. Специалисты считают, что облачные технологии со временем вытеснят классические методы работы с документами.

Рассмотрим основные преимущества, которое дает облачное хранение электронных документов для пользователей и организаций.

Одни из самых главных преимуществ – это доступность и мобильность. Доступность означает возможность получить доступ ко всем документам, файлам, папкам в облаке из любой точки мира. Конечно, при условии, что есть необходимые учетные данные и доступ в интернет. Также, не важен вид самого устройства, доступ к информации, хранящейся на облаке, можно получить с

[1] Горохов С.Н, Лобанов Е.М. Современные технологии хранения электронных документов // Вестник архивиста. 2015. № 1. С. 194.

компьютера, ноутбука, планшета или мобильного устройства, подключенного к интернету. Персонал с плотным графиком работы или те, кто живет далеко от корпоративного офиса, могут использовать эту функцию, чтобы всегда быть в курсе событий с клиентами и коллегами. Также устранена необходимость переноса файлов между устройствами, что раздражает пользователей, а также усложнят сам процесс работы с документами, т.е. есть возможность синхронизации данных. Кроме того, файлы остаются одинаковыми на всех устройствах, так как они автоматически обновляются при внесении изменений. У пользователя всегда будет последняя версия файла, независимо от того, когда и как он извлечен.

Исходя из вышеперечисленных преимуществ вытекает следующее преимущество – это расширение сотрудничества. Если в бизнесе два или более сотрудника, то сотрудничество должно стать приоритетом для компании. Облачные вычисления упрощают процесс сотрудничества. Точно так же, как раздражает передача файлов между устройствами туда и обратно, очень сложно отправлять десятки электронных писем только для того, чтобы делиться файлами. С облачным хранилищем для этого есть решение. Члены группы могут легко и безопасно просматривать, обмениваться информацией на облачной платформе. Некоторые облачные сервисы даже предоставляют совместные социальные пространства для связи сотрудников в организации, что повышает заинтересованность. Сотрудничество может быть возможным и без использования облачных вычислений, но оно будем менее упрощенным и эффективным.

Следующее преимущество – удобство использования. Пользователи могут легко перетаскивать документы и файлы в облачное хранилище. Сами данные легко сохранить в облаке, для этого не требуется никаких технических знаний. У облачных систем хранения, есть возможность легко поделиться доступом в облачной среде с другим пользователем. Данные, хранящиеся в облаке, легко и безопасно передаются клиентам и коллегам. Также облачный интерфейс для работы с документами, как правило, нагляден и интуитивно понятен, что

способствует более быстрому обучению и работе с ним сотрудников организации.

Далее можно выделить такое преимущество как экономичность. Компании и частные лица, использующие облачные службы, с большей вероятностью сократят свои эксплуатационные расходы, чем те, кто все еще использует собственные решения или внешние жесткие диски. Организация может не покупать дорогостоящие, мощные компьютеры и ПО, не создавать собственный центр обработки данных, а платить только за аренду такого оборудования, используя все мощности провайдера. Оплата при этом производится обычно раз в месяц. Также, стоит отметить, что при перемещении данных в облако, они исчезают с устройств и оборудований. То есть, данные не занимают ценное пространство дома или в офисе, потому что провайдер предлагает место для виртуального хранения. Также отпадает нужда в найме ИТ-персонала, который занимается обслуживанием СЭД.

Следующее преимущество – высокая технологичность и производительность. Как уже было сказано выше, при работе с документами используются платформа провайдера. Это позволяет использовать её для хранения и обработки своих данных с использованием всех мощностей компьютеров, поскольку облачные поставщики, как правило, используют современные высокопроизводительные оборудования и технологии, специально созданные для обработки огромного количества данных. Соответственно, облачные СЭД имеют возможность масштабируемости.

Теперь рассмотрим очень важное преимущество – контроль качества. Ущерб успеху бизнеса может нанести некачественная, непоследовательная отчетность. В облачной системе все документы должны хранится в одном месте и в одном формате. Благодаря тому, что все получают доступ к одной и той же информации, есть возможность поддерживать «непротиворечивость» своих данных, избегать человеческих ошибок и иметь четкую запись любых изменений или обновлений.

Еще одно преимущество – автоматическое обновления программного обеспечения. Для работников, полностью загруженных своей работой, раздражающим фактором может стать ожидание установки обновления системы. Облачные приложения обновляются автоматически, поэтому ИТ-отделу не нужно выполнять ручное обновление для всей организации. Это экономит драгоценное время ИТ-персонала и деньги, потраченные на консультации.

Далее рассмотрим такое преимущество как надежность и безопасность данных. Облачные сервисы, как правило, обеспечивают быстрое восстановление данных для всех видов чрезвычайных ситуаций, от стихийных бедствий до перебоев в подаче электроэнергии и сбоев в системе. Чтобы предотвратить утечку данных в облачной системе хранения документов используется резервное копирование. Стоит отметить, что клиент практически не участвует в настройке по обеспечению безопасности данных, что во-многом снижает риск ошибок. Таким образом, поломка оборудования никак не отразиться на сохранности данных, потому что информация хранится на сервере в облаке. Кроме того, дабы избежать похищения данных хакерским путем во многих облачных СЭД используется кодирование. Вид кодирования, как правило, клиент может выбрать. При этом информация кодируется еще до того, как она покинет сеть организации. Резервное копирование осуществляется после кодирования. Таким образом, облачная система работы с документами предлагает достаточно надежные решения для сохранности данных, однако, не стоит забывать, что практически любую систему защиты можно обойти.

Мы перечислили основные преимущества, которые выделяют авторы в своих работах, посвященным облачным системам электронного документооборота – это доступность и мобильность, расширение сотрудничества, удобство использования, экономичность, высокая технологичность, контроль качества, автоматическое обновление программного обеспечения, а также надежность и безопасность данных. Тем не менее, последнее преимущество остается достаточно спорным.

Идеального способа хранения электронных документов в данный момент не существует. Всегда есть вероятность информационной утечки и потери данных, вследствие взлома, поломки техники или масштабного сбоя системы. Однако системы облачного документооборота, как и сами облачные технологии сейчас находится на этапе развития и с каждым годом появляются все новые решения для их совершенствования, а также устранения ошибок.

При переходе на облачное хранение документов необходимо учитывать, что далеко не все информационные системы, использующиеся в сегодняшних компаниях, готовы и могут быть переведены в облако, а в случае некоторых такой переход просто нецелесообразен. Например, сюда можно отнести системы, простой которых может привести к катастрофическим последствиям либо потере бизнеса, например, внутренняя кооперативная система банка[1].

Поэтому, нельзя сказать, что сейчас облачная система хранения является самой оптимальной, но вполне можно предположить, что в будущем, благодаря развитию в сфере ИТ и система электронного документооборота, облачная технология заменит все традиционные методы хранения документов.

## 1.3. Недостатки использования облачных систем хранения электронных документов

В настоящее время облачные системы имеют целый ряд недостатков и недоработок. Организации, которые не учитывают риски, связанные с данной технологией, а полностью доверяют рекламным компаниям, могут подвергнуть свой бизнес опасности.

Поскольку технология находится еще на стадии развития, облачным вычислениям еще далеко до эталонной модели такой системы. Создание новых стандартов, в том числе для обеспечения безопасности облачных технологий, на

[1] Шпарло. Е.В. Возможности облачных технологий для хранения документов: за и против // Современный документооборот. 2015. № 7. С. 215.

сегодняшний день является приоритетной задачей в области ИТ, облачные решения будут развиваться вместе с возникновением новых, более надежных способов хранения и обработки данных.

Многое зависит от того, кто именно предоставляет облачные услуги. Если провайдер надежно защищает данные клиента, делает их резервные копии, осуществляет шифровку, при этом работает несколько лет на рынке и имеет хорошую репутацию, то угрозы безопасности данных может никогда не произойти. Как сказал известнейший специалист по криптографии и компьютерной безопасности Брюс Шнайер, весь вопрос в доверии[1].

Рассмотрим подробно основные недостатки и риски, связанные облачными системами хранения электронных документов:

1. Полная зависимость клиента от Интернета. Любой сбой в интернете приводит к ограничению, а то и к полной остановке доступа пользователя к данным, что может серьезно замедлить работу организации. Однако, этот недостаток не так существенен, т.к. проблемы с интернет соединением в настоящее время не часты. Что касается потери данных при отключении интернете, решением может стать резервное копирование данных, предоставляемое большинством провайдеров.

2. Технические неполадки и сбои в системе. Любая информационная технология всегда подвержена сбоям и другим техническим проблемам. Одна из возможных проблем в работе с облачным оборудованием – есть вероятность, что облачном сервисе может произойти поломка, которая приведет к сбою всей системы. Несмотря на то, что случается такое нечасто, в облачных центрах есть примеры ошибок, приводящих к поломке серверов.

Многие сервисы облачного хранения имеют встроенные функции безопасности, благодаря чему, даже не имеют сбоев в истории работы своей системы. Но даже если после поломки данные можно будет восстановить,

---

[1] Лященко Ю.В. Преимущества и недостатки облачных технологий. Актуальные проблемы авиации и космонавтики. 2014. № 8. С. 383.

например, с помощью резервного копирования, такой сбой на длительное время приостановит работу офиса или организации, что может привести к простоям.

3. Отсутствие контроля за данными. Преимущество, благодаря которому клиенту не нужно тратить время и ресурсы на обслуживание и контроль своего облака является также серьезным недостатком. Заказчик может контролировать и управлять только приложениями, данными и службами, работающими поверх системы, но не управлять самой внутренней инфраструктурой.

Предприятия также могут столкнуться с потерей контроля над конфиденциальными данными. Проблема здесь заключается в том, что при использовании сторонних служб обмена файлами данные обычно извлекаются за пределы ИТ-среды компании, а это означает, что настройки конфиденциальности данных находятся вне контроля предприятия. А поскольку большинство облачных сервисов использует резервное копирование своих данных в режиме реального времени, многие данные, которые не предназначены для совместного использования, могут в конечном итоге просматриваться неавторизованным персоналом. Лучший способ избежать такого риска - убедиться, что провайдер зашифровывает файлы организации во время хранения.

4. Пожизненные расходы. Удобство одной низкой ежемесячной арендной платы сначала выглядит привлекательно, особенно для компаний на старте своего бизнеса. Однако, при использовании общедоступного облачного хранилища цена в течении многих лет может заметно возрасти.

Кроме того, если подсчитать все расходы в течение трех, четырех или пяти лет за аренду облачного сервера для работы с документами, то остается вопросом - будет ли это действительно дешевле использования своего оборудования и локальной сети.

5. Ограниченная пропускная способность. Не все облачные провайдеры созданы одинаково. В идеале стоит пользоваться услугами поставщика, предлагающего неограниченную пропускную способность. Предложения SaaS, как правило, начинаются с бесплатного пакета, но потом возникает

необходимость платить за дополнительное место и новые предложения. Не известно сможет ли бизнес компании позволить себе расходы по мере расширения и роста своих потребностей.

5. Киберпреступность. Файлы в облаке являются одними из наиболее уязвимых для взлома, если провайдер не соблюдает меры безопасности. Тот факт, что они хранятся и передаются через Интернет, является основным фактором риска. И даже если облачный сервис обеспечивает шифрование файлов, данные все равно могут быть перехвачены на пути к месту назначения. Наилучшей формой защиты от этой угрозы было бы обеспечение того, чтобы данные шифровались и передавались по защищенному соединению, это предотвратит доступ посторонних к метаданным облака.

6. Вероятность потери данных. Как хорошо известно, в Интернете нет ничего абсолютно надежного и безопасного, следовательно, всегда есть вероятность потери конфиденциальных данных не обязательно преднамеренно. Причинами потери ценной информации могут быть ошибки в работе провайдера, халатность сотрудников и недолжное соблюдение мер безопасности по защите данных, как со стороны поставщика, так и со стороны клиента.

Таким образом мы рассмотрели основные недостатки использования облачных систем хранения электронных документов, мы выделили полную зависимость клиента от Интернет-соединения, технические неполадки и сбои в системе, отсутствие контроля за данными, пожизненные расходы, ограниченную пропускную способность, киберпреступность и вероятность потери данных.

Каждое из этих недостатков следует учитывать при выборе облачного хранилища или службы онлайн-резервного копирования для работы с документами. Надо сказать, что не все из перечисленных аспектов являются серьезной проблемой. Большинство облачных компаний нашли способы разрешить их тем или иным образом. Клиент в праве сам проанализировать подходящие ему предложения облачных серверов для работы с документами и выбрать из них самый оптимальный, учитывая инфраструктуру и бюджет своей организации.

В настоящий момент, облако не реализуется в одночасье. Организациям решившим таким образом оптимизировать свой электронный документооборот, предстоит проделать сложную работу. Стратегический подход, детализация управления и участие профессионалов в сфере ИТ могут помочь снизить потенциальные риски, затраты и недостатки в процессе внедрения.

Таким образом, подводя итоги главы, составим таблицу, где мы можем сравнить между собой преимущества и недостатки использования облачных технологий хранения.

Таблица 1 – Сравнительная характеристика функциональных аспектов облачных технологий хранения документов

| Характеристика аспекта | Преимущество | Недостаток |
|---|---|---|
| Затраты на программное обеспечение | Предприятия и организации часто могут сократить годовые эксплуатационные расходы за счет использования облачного хранилища, для пользователей - это дополнительная экономия средств, поскольку она не требует внутренних ресурсов организации для хранения информации удаленно. | Если пользователь желает локально управлять всеми ресурсами и возможностями облачного хранилища, необходимо создание внутри организации частного облака – установка необходимого дополнительного ПО на все необходимые устройства, что будет намного дороже в цене. |
| Безопасность и восстановление данных | В облачное хранилище может использоваться резервное копирование, предоставляющее копию важных файлов. Эти файлы хранятся в удаленном месте и могут быть доступны через Интернет. | Технические сбои и обновления программного обеспечения облачных хранилищ, вредоносные программы и кибератака могут спровоцировать утечку важной информации. |
| Пропускная способность | Вместо отправки самих файлов отдельным лицам можно отправлять электронную ссылку на документ получателям по электронной почте, тем | Некоторые облачные хранилища имеют ограниченную пропускную способность. Если организация превышает оговоренный лимит |

| Характеристика аспекта | Преимущество | Недостаток |
|---|---|---|
| Удобное использования и доступность | Все облачные службы позволяет пользователям перемещать файлы между облачным и локальным хранилищем в любое удобное время. Все необходимые файлы можно получить из любого места через Интернет. | Если подключения к Интернету отсутствует по каким-либо причинам, у пользователя не будет доступа к данным. |

# 2. ЗАЩИТА ДАННЫХ В ОБЛАЧНЫХ СИСТЕМАХ РАБОТЫ С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

## 2.1. Проблемы защиты данных в облачных системах работы с электронными документами

Технологии защиты данных с каждым годом становятся все более востребованными в связи с распространенностью и ростом киберпреступности. Чем больше ИТ-специалистами разрабатывается более сложных и хитрых методов защиты информации, тем больше возникает новых видов атак, которые обходят современные средства защиты и ставят под угрозу всю безопасность компании.

Для российских организаций вопрос защиты электронных документов – один из краеугольных, особенно с учетом Федерального закона № 152 «О персональных данных». Безопасность – это «ахиллесова пята» облачных решений[1].

Облачные системы работы с документами являются гибкими и масштабируемыми, обладают большим пулом вычислительных ресурсов. Из-за расширенного функционала облака, злоумышленники могут использовать его не по назначению. Это вызывает различные проблемы с безопасностью облачных вычислений.

Из опроса SAP СНГ за февраль 2017 года следует, что основное недоверие к облачным системам работы с документами связано именно с проблемой защиты данных. В опросе принимали участие малые, средние и крупные российские предприятия в сфере бизнеса[2]. Данные опроса отображены на Рис. 4.

---

[1] Гусеев А.В. Перспективы облачных вычислений и информатизация учреждений здравоохранения // Медицинские информационные системы. 2011. № 2. С. 9.

[2] Суханов В.И. Облачный сервис хранения данных // Научный журнал КубГАУ. 2013. № 8. С. 20.

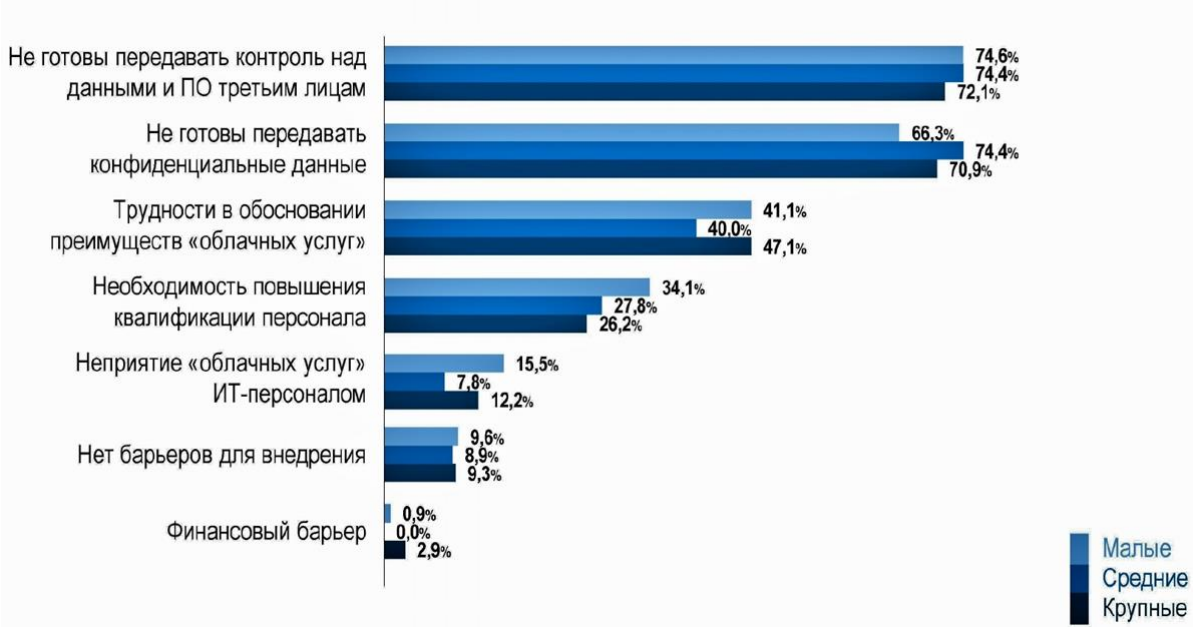


Рисунок 4 – Основные барьеры для внедрения облачных услуг[1]

Кроме того, вопросы безопасности информации в облаке касаются не только частных бизнес-организаций. Защита данных в облачной системе электронного документооборота – это актуальная проблема для государственных и муниципальных предприятий России.

В современной России наблюдается процесс активного внедрения в систему государственного управления информационно-коммуникационных технологий, на базе которых образуется новая форма взаимодействия государства с бизнесом, гражданами, общественными объединениями и негосударственными некоммерческими организациями[2].

Динамично развиваются веб-сайты федеральных, региональных и муниципальных органов власти, объединенные в единый правительственный интернет-портал. Внедряются системы «Электронное муниципальное управление», «Электронное государственное управление регионом» и т.д[3].

---

[1] Суханов В.И. Облачный сервис хранения данных // Научный журнал КубГАУ. 2013. № 8. С. 20.

[2] Овчинников С.А. Облачные технологии как фактор политического риска электронного государственного управления // Автоматика. Вычислительная техника. 2012. № 4. С. 187.

[3] Там же. С. 188.

В связи с активной «интернетизацией» государственных структур, в будущем возможно повсеместное использования облачных систем электронного документооборота.

Таким образом, эффективность государственного управления может напрямую зависеть от информационных технологий, которые используют государственные предприятия для работы с документами. Следовательно, защиту данных в современных ИТ-технологиях документооборота можно рассматривать как фактор политического риска в нашей стране.

Проблемы безопасности, связанные с облачными вычислениями, делятся на две широкие категории: проблемы безопасности, с которыми сталкиваются поставщики облачных услуг и проблемы безопасности, с которыми сталкиваются их клиенты. Однако ответственность распределяется. Поставщик должен обеспечить безопасность своей инфраструктуры и защиту данных приложений своих клиентов, в то время как пользователь должен принять меры для укрепления своего приложения, использования надежных паролей и мер аутентификации.

Рассмотрим подробно основные проблемы защиты данных в облачных системах работы с электронными документами.

Данные в руках разработчика. Основной особенностью, подвергающейся постоянной критике является то, что при использовании виртуального программного обеспечения (ПО) данные автоматически попадают в руки разработчика этого ПО. Последнее время, касаемо облачных сервисов, стал популярен лозунг «это не облако, а просто чей-то компьютер». Большинство компаний, которые отказались от использования облака, сделали это из-за страха утечки своих данных[1]. То есть, данные могут подвергаться риску неправильного обращения со стороны поставщика. Лучшая стратегия заключается в том, чтобы зависеть от шифрования файлов и более надежных паролей, а не от самих поставщиков облачных услуг. У большинства приличных компаний облачных

[1] Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. № 6. С. 30.

хранилищ должны быть гарантированные протоколы по защите данных. Также, в некоторых облачных системах появились очень надежные способы защиты информации, например, способ под названием «принцип нулевого разглашения», основанный на постоянном шифровании. Суть этой защиты сводится к тому, что только у организации есть ключ доступа к данным. То есть, даже сам поставщик облачной услуги не будет иметь права доступа к системе.

Кибератака (DDoS-атаки, спуфинг, фишинг и др.). Кибератаки в наше время – одна из важных проблем и облачная система к ним крайне уязвима. Часто встречающимися, но в тоже время характерными угрозами для облачной технологии являются DDoS-атаки, перехват личных данных для доступа к облаку через его API, несанкционированный захват данных, отправляемых и получаемых из облака, а также взлом целостной среды. Для минимизации рисков и профилактики подобных угроз поставщики облачных услуг используют продвинутые средства безопасности. Но помимо современных решений, требуется понимание сущности и природы такого вида атак[1].

Небезопасный интерфейс. Интерфейс облачной системы – важная составляющая программного обеспечения облака, с которой постоянно взаимодействует пользователь. От того, насколько хорошо проработаны механизмы интерфейса облачной системы зависит безопасность данных. Для защищенной работы с программой, поставщик должен уделить внимание механизму контролю доступа к системе, идентификации и аутентификации пользователя.

Потеря данных или утечка. Документы, хранящиеся в облаке, могут быть утеряны и без кибератак. Случайное удаление данных поставщиком облачных услуг или физическая катастрофа, например, пожар или землетрясение, может привести к необратимой потере данных клиента. При этом вина может лежать не только на плечах провайдера. Если клиент зашифровывал свои данные перед

[1] Малков В.В. Защита информации в облаках для предпринимательского сектора // Вестник Московского государственного университета печати. 2015. № 15. С. 88.

загрузкой в облако, но потерял свой ключ шифрования, то информация может быть безвозвратно утеряна.

Правительственное вторжение. Политическая ситуация в России последние несколько лет нестабильна. Блокировка правительством иностранных Интернет-ресурсов возможна любое время и нет никаких гарантий, что этого не произойдет. Точный прогноз такого события составить невозможно. Вполне, может возникнуть неожиданная ситуация, к примеру, правительство может заблокировать какой-либо иностранный сервис для русских пользователей, а ведь некоторые отечественные облачные системы электронного документооборота используют иностранные облачные платформы для хранения данных своих клиентов. Кроме того, данные своего клиента может предоставить сам провайдер вследствие государственного давления на него.

Технология общего пользования. Принцип работы в облачной среде - это общий пул ресурсов, т.е. провайдер предоставляет универсальную виртуальную инфраструктуру для множества пользователей. Неправильная конфигурация может привести к компрометации всего облака. Следовательно, если на одном из уровней возникает ошибка, это влияет на всю систему.

Кража учетных записей. Взлом учетной записи в облаке – это процесс, при котором злоумышленник похищает или захватывает учетную запись отдельного лица или организации. Это распространенная тактика в схемах кражи личных данных, когда злоумышленник использует украденную информацию учетной записи для осуществления злонамеренной или несанкционированной деятельности. Как только информация для входа в систему или другая конфиденциальная информация получена, злонамеренный пользователь может легко проникнуть в систему, поскольку сама система доступна из любого места. При захвате учетной записи в облаке, злоумышленник обычно использует взломанную электронную почту или другие учетные данные, чтобы выдать себя за владельца учетной записи. В основном, такие проблемы являются результатом неправильного обращения с механизмами защиты, например, если используются

слабые пароли, управление ключами шифрования происходит ненадлежащим образом и др.

Злоупотребление облачными сервисами. Пользоваться облачными услугами могут нелегитимные организации. Их цель – использовать облачные системы для своих злонамеренных действий – рассылка спама, DDoS-атаки, запуск вредоносных программ и др. Провайдером необходимо распознавать подобных пользователей – изучать трафик, производить мониторинг облачной системы и т.д.

Злоумышленники среди сотрудников поставщика. Даже если сам провайдер услуг не имеет намерения вредить своему клиенту, под его управлением может работать сотрудник, который обрабатывает информацию пользователей. Такой сотрудник может в корыстных целях тайно использовать данные клиента.

Халатность сотрудников поставщика. Ошибки сотрудников остаются одной из самых больших проблем безопасности для всех систем, но эта угроза особенно опасна для облачных решений. Сотрудники могут подключаться к облачным решениям со своих мобильных телефонов, домашних планшетов и домашних ПК, что потенциально делает систему уязвимой для многих внешних угроз.

Отсутствие необходимых мероприятий по защите со стороны пользователя. Клиент облачных систем также должен принимать участие в обеспечении безопасности свои данных. Если офис и персональные компьютеры организации не защищены от проникновения посторонних лиц, то вина за утечку информации будет лежать на клиенте. К обязательным мероприятиям также относятся обучение сотрудников безопасной работе с системой, мониторинг ошибок системы, тестирование на проникновение угроз и т.д.

Таким образом, облачные вычисления сталкиваются со многими проблемами безопасности как на стороне поставщика услуг, так и на стороне клиента. Основными проблемами являются нахождение данных в руках разработчика, кибератаки, небезопасный интерфейс, потеря данных или утечка,

правительственные вторжения, принцип технологии общего пользования, кража учетных записей, злоупотребление облачными сервисами, злоумышленники среди сотрудников поставщика, халатность сотрудников поставщика, отсутствие необходимых мероприятий по защите со стороны пользователя.

Полноценная защита данных и полное соответствие требованиям ФЗ № 152 – задача не из легких и не дешевых. Размещение базы данных предприятия с его секретной документацией в облаке – шаг достаточно рискованный, требующий всестороннего анализа таких рисков и создания надежной системы защиты.

## 2.2. Методы защиты данных в облачных системах работы с электронными документами

Безопасность облачных вычислений относится к широкому набору политик, технологий, приложений и элементов управления, используемых для защиты виртуализированных IP, баз данных, приложений, услуг и инфраструктуры облачных вычислений. Защита облачных систем – это часть компьютерной безопасности, сетевой безопасности и, в более широком смысле, информационной безопасности.

Защита данных является одним из наиболее важных аспектов в проблеме безопасности облачных систем работы с документами. Чтобы повысить безопасность облачных сред предприятиям необходимо использовать современные технологии и передовые методы для защиты своих данных.

Облачная система безопасности эффективна только при наличии правильных методов защиты. Архитектура облачной СЭД должна распознавать проблемы, возникающие при управлении безопасностью[1]. Управление безопасностью решает эти проблемы с помощью средств управления

[1] Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. № 6. С. 35.

безопасностью. Эти элементы управления введены в действие, чтобы защитить любые слабые места в системе и уменьшить эффект кибератак.

Облачные сервисы имеют высокую безопасность при должном ее обеспечении, однако при халатном отношении эффект может быть полностью противоположным. Решением является соответствие облака требованиям нормативных документов и стандартов в области обеспечения информационной безопасности.

В российском законодательстве пока нет стандартов, описывающих принцип построения защиты информации в облачных технологиях. Вследствие этого поставщики облачных услуг вынуждены сами выбирать способы защиты информации из огромного количества готовых решений, представленных на рынке. Но все средства защиты должны учитывать особенности облачной технологии[1].

Рассмотрим основные виды угроз информации в облачных системах работы с документами.

Е.А. Догваль[2] в своей научной статье выделяет пять основных видов угроз облачных сервисов:

1. Традиционные атаки на программное обеспечение. Связаны с уязвимостью применяемых сетевых протоколов, операционных систем, модульных компонентов и т.д.

Для защиты от таких атак применяют антивирусные программы, межсетевой экран (файервол), систему предотвращения вторжений (Intrusion Prevention System) и др.

2. Функциональные атака на элементы облака. Такие атаки связаны с многослойностью облака. Основным средством обороны от подобных кибератак выступает защита самого слабого места системы.

---

[1] Хажиева А.С. Принципы защиты информации в облаке // Информационная безопасность. 2016 № 9. С. 10.

[2] Е.А. Догваль. Методы повышения безопасности в сфере «облачных» технологий // Вестник АГУ. 2014. №4. С. 170.

Для защиты от функциональных атак для каждого слоя облака нужно использовать для каждого из них специальные средства защиты: для прокси – защиту от DDoS-атак, для веб-сервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для слоя СУБД – защиту от SQL-инъекций, для системы хранения – резервное копирование и разграничение доступа[1].

3. Атаки на клиента. Этот тип атак очень распространен в веб-пространстве. Такие атаки также характерны для облачных систем, поскольку пользователи обычно получают доступ к облаку через веб-браузер. К этим видам атак относятся межсайтовый скриптинг, кража паролей, перехват веб-сессий, атака посредника и др.

В качестве защиты здесь традиционно используется аутентификация пользователя, в том числе эффективная двухфакторная аутентификация, шифрованное соединение с взаимной аутентификацией[2].

4. Атаки на средства виртуализации. К ним относятся атаки на гипервизор, на виртуальные машины при взаимодействии между узлами облака, а также атаки на системы управления облаком.

Такие угрозы в настоящее время крайне редки, сведения о подобных реальных атаках отсутствуют. Однако, их стоит иметь в виду, поскольку они могут появиться в будущем в связи с популярностью виртуализации облаков[3].

5. Комплексные угрозы облачных сервисов. Причины такой угрозы – неправильный контроль инфраструктуры. Нет никаких гарантий, что все ресурсы облака посчитаны и в нем нет неподконтрольных виртуальных машин, не запущено лишних бизнес-процессов и не нарушена взаимная конфигурация слоев и элементов облака. Этот тип угроз связан с управляемостью облаком как единой информационной системой и поиском злоупотреблений или других

---

[1] Е.А. Догваль. Методы повышения безопасности в сфере «облачных» технологий // Вестник АГУ. 2014. № 4. С. 171.

[2] Кодлов П.А. Проблемы безопасности облачных вычислений // Наука, техника и образование. 2016. № 12. С.56.

[3] Гладкий М.В. Безопасность приложений на платформах облачных вычислений // Труды БГТУ. 2015. № 9. С 205.

нарушений в работе облака, которые могут привести к излишним расходам на поддержание работоспособности информационной системы.

Этот тип угроз более сложный и для него нельзя назвать универсальный способ защиты – методы безопасности в таком случае разрабатываются персонально для каждого облака.

Итак, проанализировав различные источники, посвященные безопасности данных в облачных технологиях работы с электронными документами можно выделить следующие эффективные методы защиты данных в облачных технологиях работы с электронными документами:

1. Шифрование данных. Шифрование – один из самых эффективных методов защиты информации. Провайдер должен шифровать данные пользователя со стороны сервера, который находится в центре обработки данных. Существует несколько методов шифрования данных при использовании облачного хранилища. Шифрование на стороне сервера – шифрование, которое происходит после того, как система получает как данные, но до того, как данные записываются на диск и сохраняются, а также шифрование на стороне клиента – шифрование, которое происходит перед отправкой данных в облачное хранилище. Такие данные поступают в облачное хранилище уже в зашифрованном виде, но также подвергаются шифрованию на стороне сервера.

Важным остается вопрос о ключах шифрования. Хранить их на сервере облака не разумно, т.к. любой, у кого есть доступ к этому серверу, мог бы получить доступ к ключу, а значит и к зашифрованной информации. Физический ввод ключа заменяется запросом, который облачный сервер отправляет внешнему источнику – серверу управления ключами

Важной составляющей для реализации такой защиты является раздельная эксплуатация облачного сервера и сервера управления ключами: если оба размещены у одного и того же провайдера облачных сервисов, то вся информация снова оказывается собранной в одном месте. Хорошей альтернативой является установка сервера управления ключами в локальном

центре обработки данных или в качестве внешней услуги у другого сервис-провайдера[1].

2. Защита данных при передаче. Для безопасной обработки данных обязательным условием является их шифруемая передача. В целях защиты данных в публичном облаке используется туннель виртуальной частной сети, связывающей клиента и сервер для получения публичных облачных услуг. Туннель виртуальной частной сети способствует безопасным соединениям и позволяет использовать единое имя и пароль для доступа к разным облачным ресурсам. В качестве средства передачи данных в публичных облаках VPN - соединение использует общедоступные ресурсы, такие как Интернет. Процесс основан на режимах доступа с шифрованием при помощи двух ключей на базе протокола Secure Sockets Layer (SSL)[2]

3. Аутентификация. Аутентификация – это защита паролем. Например, используют токены. Токен – это электронный ключ, используемый для обеспечения информационной защиты, а также для идентификации пользователя. В системе аутентификации используют также концепцию одноразовых паролей. Такие пароли, могут использоваться только для одного сеанса аутентификации, могут быть ограничены определённым промежутком времени.

Основное отличие облачной инфраструктуры заключается в большой масштабируемости и более широкой географической распределенности. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису.

---

[1] Хажиева А.С. Принципы защиты информации в облаке // Информационная безопасность. 2016 № 9. С. 11.

[2] Там же. С. 12.

Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и аутентификацию SAML (Security Assertion Markup Language)[1].

4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service).

Часто провайдеры изолируют данные пользователей друг от друга за счет изменения кода в единой программной среде. Этот подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющем получить доступ к данным. В случае возможной ошибки в коде пользователь может получить доступ к информации другого пользователя.

Говоря о защите данных в облачных системах работы с документами, нельзя также не упомянуть про сам центр обработки данных. Под центром обработки данных подразумевается совокупность серверов, размещенных на одной площади с целью повышения эффективности и защищенности.

Подсистема обеспечения безопасности центров обработки данных должна включать в себя следующие элементы[2]:

- охранное видеонаблюдение;
- охранно-пожарная сигнализация;
- система контроля и управления доступом;
- система резервного копирования и восстановления данных;
- система защиты информации в центре обработки данных.

Помимо технологий защиты информации с точки зрения провайдера, также важны методы предупреждения проблем со стороны клиента.

---

[1] Хажиева А.С. Принципы защиты информации в облаке // Информационная безопасность. 2016 № 9. С. 15.

[2] Ивонин П.В. Безопасность облака в деталях // Известия ЮФУ. 2013. № 2. С. 36.

Проанализировав различную литературу, мы можем разработать рекомендации пользователям облачных сервисов для обеспечения безопасности и сохранности их данных:

1. Провести анализ облачного рынка. Важно понять, какие облачные системы хранения существуют на предприятиях, кто их использует и каким образом. Доверять свои данные можно только надежным и проверенным компаниям, зарекомендовавшим себя на рыке. Чтобы не ошибиться в выборе, нужно учесть такие немаловажный факторы как репутацию облачного сервиса, срок его работы, отзывы клиентов, а также его популярность.

2. Определить, как поставщик облачного хранилища решает вопросы конфиденциальности и безопасности. Условия соглашений об обслуживании – хорошая отправная точка для определения общих мер защиты, предлагаемых облачным провайдером. Но этого недостаточно для обеспечения безопасного хранения файлов. Поставщики облачных услуг часто обновляют условия обслуживания и пользовательские соглашения. Из-за этого можно легко пропустить незначительными изменения, которые могут оказать существенное влияние на конфиденциальность и безопасность.

Большинство соглашений не охватывают детали того, как поставщик облачного хранилища реализует безопасность, какие конкретные методы защиты он использует и что происходит в случае поломки или нарушения. В результате важно точно определить политику и процедуры, что будет способствовать дальнейшим переговорам с провайдером.

2. Знать какие средства защиты должны применяться. Шифрование в облачной среде является фундаментальным требованием. Важно знать, как поставщик облачного хранилища использует шифрование, в том числе при передаче данных между центрами обработки данных, серверами и устройствами хранения, а также кто контролирует ключи шифрования, как они применяются к конкретному набору данных.

Организация, использующая облачного провайдера, должна знать, у кого есть доступ к системам, какие существуют другие средства защиты – от DDoS-атак до системных ошибок в приложениях.

3. Использовать многофакторную аутентификацию на всех устройствах и системах. Широкое использование многофакторной аутентификации во много раз снижает риск получения доступа к системе или приложению для выпуска вредоносных программ или похищения ценной информации. Многофакторная аутентификация может помочь в защите конфиденциальных данных от хакеров, недовольных сотрудников и других инсайдеров, которые могут преднамеренно или непреднамеренно подвергать данные риску.

4. Проводить аудит и тестирование на проникновение угроз. Независимо от того, сотрудничает ли компания со сторонней фирмой по безопасности или полагается на внутренний персонал своей организации – эксперты считают, что необходимо провести тестирование на проникновение угроз, чтобы определить, правильно ли разработаны меры по облачной безопасности системы.

Организация должна регулярно проводить аудит возможностей облачной безопасности системы. Аудит должен включать анализ возможностей поставщиков, методы защиты должны соответствовать условиям безопасности.

Также для обеспечения безопасности следует проверять свои журналы доступа, дабы убедиться в том, что только авторизованные сотрудники имеют доступ к конфиденциальным данным и приложениям в облаке.

5. Обеспечить физическую защиту своих данных. Физическая защита данных предполагает минимизирование рисков, связанных с проникновением посторонних лиц к компьютерам организации. Кроме, контроля входящих и выходящий посетителей, стоит также закрывать кабинет на ключ и обязательно блокировать компьютер перед уходом.

Таким образом, мы рассмотрели основные методы защиты данных облачной системе работы с электронными документами, а также разработали рекомендации мер безопасности для пользователей таких систем.

В большинстве случаев проблемы с безопасностью не должны мешать организациям использовать облачные сервисы. Следуя рекомендациям по облачной безопасности, они могут еще больше снизить риск таких угроз, пользуясь при этом все преимуществами облачных вычислений.

Как большие, так и малые организации тратят приличные ресурсы на разработку и усовершенствование систем защиты своих облачных продуктов. Выбирая облачный сервис, необходимо внимательно изучить все его характеристики, особенно это касается вопроса надежности.

В настоящее время методы защиты информации в облачных сервисах нуждаются в новом подходе. Защита должна включать целый комплекс мер, реализуемый с помощью слаженной работы поставщика и пользователя услуг.

Для реализации проекта еще на этапе его проработки нужно подключать профессиональных специалистов по безопасности, с помощью которых прорабатывать и предусматривать соответствующие программно-аппаратные средства защиты, включая надежное шифрование, ограничение доступа к серверному оборудованию надежное протоколирование работы, регламентированный доступ на основе групповых политик и т.д[1].

## 2.3 Применение облачных технологий в электронной подписи

Одни из самых важных аспектов электронного документооборота – это задача идентификации пользователя, придание юридической силы, а также защиты электронного документа. Именно с целью решения этих вопросов была разработана электронно-цифровая подпись (ЭЦП).

ЭЦП – технология, позволяющая подтвердить авторство электронного документа, т.е. ЭЦП является реквизитом электронного документа. В её основе лежит криптографический метод защиты информации. Различают три вида ЭЦП

[1] Гусеев А.В. Перспективы облачных вычислений и информатизация учреждений здравоохранения // Медицинские информационные системы. 2011. № 2. С. 13.

– простые, усиленные неквалифицированные и усиленные квалифицированные электронные подписи.

Использования ЭЦП уже давно воплощено в жизнь, почти все организации приобретают электронную подпись для функционирования своей деятельности. На сегодняшний день существует ряд нормативных документов, которые определяют работу ЭЦП:

1. Федеральный закон №63-ФЗ «Об электронной подписи»[1] от 06.04.2011, описывающий и регулирующий отношения в области использования электронных подписей.

2. Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] от 27.07.2006, в котором даются понятия электронного документа. Этот закон регулирует отношения, возникающие при распространении информации, применении информационных технологий и обеспечении защиты информации.

3. Федеральный закон №149-ФЗ «О бухгалтерском учете»[3] от 06.12.2011, где прописаны требования в бухгалтерским электронных документов.

4. Пункт 3 статьи 75 Арбитражного процессуального кодекса РФ, который гласит, что документы, подписанные электронной подписью, допускаются в качестве письменного доказательства.

В сфере ИТ сейчас говорят о новой технологии электронной подписи – облачной подписи. Появилась она в связи с тем, что многие организации стали переходить на облачные системы для реализации своего электронного документооборота.

Технология облачной подписи активно развивается в России. В данный момент рассматриваются проекты федерального закона, вносящих изменения в

---

[1] Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ.-[Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ. [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

[3] О бухгалтерском учете. Федеральный закон от 06.12.2011 №149-ФЗ. [Электронный ресурс]. Режим доступа http://www.consultant.ru/document/ cons_doc_LAW_122855

подписание электронных документов, возможности создания доверенности в электронном виде, а также возможности применения и регламентации облачной электронной подписи.

В 2017 компания 1С-СП, которая является дочерним предприятием компании 1С, выпустила SIM-карты для телефона, которые позволяют подписывать свои документы с помощью облачной ЭП со смартфона. Также в 2017 Компания «Крипто-Про», которая занимается разработкой криптографических программ для электронных подписей, выпустила сервис квалифицированной электронной подписи в облаке «КриптоПро DSS» и совсем недавно получила сертификацию.

Массово облачная подпись распространена, например, в банковской сфере. Сервис E-invoicing использует облачные технологии для согласования и передачи электронных документов и имеет при этом все необходимые лицензии. Этот сервис доступен в «Сбербанк Бизнес Онлайн». Им пользуются также многие известные компании: Metro, Лента, Ашан, Дикси, OBI, Перекресток и другие.

Возникновение облачной ЭЦП произошло в 2010 году, когда предприятия искали решения для работы с электронной подписью в облачной среде. В основном это было связано с электронным правительством. В тот момент обсуждался более удобный способ хранения ключей ЭЦП, что дало начало развития технологии облачной подписи.

Обозначим понятие облачной электронной подписи.

Облачная электронная подпись – это сервис, представляющий возможность подписывать документы, используя секретный ключ ЭП, распложенный в облаке, доступ к которому возможен множеством способов – от входа через WEB-браузер и запуска программ для настольного персонального компьютера (ПК) до использования мобильного приложения для смартфонов и планшетов[1].

[1] Саломаха Н.А. Угрозы информационной безопасности при использовании облачных электронных подписей // Безопасность информационной среды. 2017. № 14. С. 216.

Секретный ключ хранится в самом облаке, вся остальная инфраструктура – это средства организации безопасного доступа владельца ключа ЭП к данному сервису. Сам процесс подписания документа и его шифрования так же происходит на защищенном сервере.

То есть, облачная ЭЦП обладает такими же свойствами и преимуществами, как и обычная электронная, различие только в способе хранения – она хранится не на USB-носителе или компьютере, а на облачном защищенном сервере.

Облачная подпись решает многие проблемы стандартной ЭЦП. Рассмотрим основные преимущества облачной подписи по сравнению с обычной ЭЦ.

Традиционный способ хранения ключа ЭЦП – на USB-носителе, жестком диске или реестре операционной системы. В этом есть неудобства. К примеру, при подписании всегда необходимо носить с собой USB-устройство, на котором хранится электронная подпись. Основной недостаток здесь – физический риск, потому что такой носитель всегда можно потерять или забыть. Возможна также кража носителя, злоумышленник в таком случае получит от имени владельца совершать любые операции, возможные с использованием этой ЭЦП.

Как уже говорилось раннее, облачная подпись хранится в облаке, это делает её более гибкой. С помощью облачной подписи документ можно подписать в любом месте, из любой точки планеты и даже с любого устройства, используя только веб-браузер для подключения, в отличии от обычной электронной подписи.

Также одна из проблем стандартной ЭЦ – возможная несовместимость программного обеспечения устройства, с которого подписывается электронный документ. Например, под разные версии Windows нужно устанавливать соответствующие ему ПО и версии драйверов. Если разработчик не поддерживает другие версии операционной системы, то подписать документ в такой системе будет невозможно. К этой проблеме можно отнести также владельцев Apple и ноутбуков Macbook, для которых нет ПО, обеспечивающего создание электронной подписи в операционной системе Mac. Что касается

облачной подписи – её подписание и шифрование осуществляется на сервере, поэтому для этого не требуются дополнительное ПО.

Облачную подпись можно использовать не только в онлайн режиме. Возможно её применение оффлайн, поэтому неполадки с интернетом не станут основной проблемой при её использовании. При возникновении проблем с сетью, документ может быть подписан в режиме оффлайн и, после того как доступ к сети снова возобновиться, документ будет отправлен. Кроме того, облачная подпись обойдется дешевле, чем обычная, т.к. не находится на переносном физическом носителе.

Теперь поговорим о недостатках облачной подписи. Все, что касается её недостатков относится в основном к вопросам безопасности.

По сути процесс подписания (физически) происходит через удостоверяющий центр. То есть, конфиденциальная информация ключа находится на сервере удостоверяющего центра. Это спорный недостаток, который больше относится к вопросу доверия. То есть, если клиенту необходимо именно самому подписывать документ, то облачная подпись ему не подойдет. Тем не менее, удостоверяющие центры, как правило, имеют все необходимые ресурсы для защиты информации, поэтому можно рассматривать это также, как и преимущество.

Кроме того, в данный момент времени использовать облачную подпись можно только там, где есть интеграция ПО с удостоверяющим центром. Плагины во многих предприятиях не работают с облачной подписью. Порталы только планируют настраивать интеграцию с облачной подписью. Переход займет много времени. По этой причине облачная подпись не используется сейчас повсеместно в России.

Стоит также сказать, что мобильные устройства, с помощью которых используется облачная ЭП, нельзя назвать надежными. В настоящее время существует множество вредоносных программ, созданных для атаки мобильных устройств. Использования одноразового СМС-пароля для входа способствует решению такой проблемы, однако, СМС-сообщение также можно перехватить.

Проанализировав различные источники, посвящённые безопасности данных с облачными подписями, мы можем разработать рекомендации для пользователей облачной электронной подписи:

1. Обязательная установка антивирусной программы для устройств, на которых выполняются операции с облачной подписью. Выбрать нужно надежный, зарекомендовавший себя на рынке, антивирус, учитывая при этом его дополнительные опции контроля. Такой простой шаг поможет избежать многих проблем с кибератаками.

2. Не использовать опцию автоматического сохранения логина и пароля в браузере. Такая функция доступна во многих популярных веб-браузерах и, действительно, эта функция является удобной, но, к сожалению, совершенно не безопасной. Перехватив эти данные с браузера, злоумышленник сможет легко войти в личный кабинет пользователя.

3. Удостоверится, что при авторизации пользователя к облачному сервису используется защищенный протокол HTTPS. Он используется для шифровки данных с целью повышения безопасности соединения.

4. Удостоверится, что на смартфоне или планшете, используемом при работе с облачной ЭП, отсутствует неофициальная прошивка. На такой прошивке могут быть недоработки или умышленные упущения, которые сможет использовать злоумышленник для взлома. Чтобы этого избежать пользоваться нужно только официальными прошивками версий от производителя.

5. Не устанавливать на свое устройство большое количество разных приложений, особенно – из неизвестных источников. По возможности лучше иметь минимальное количество приложений, скаченных с интернета.

6. Нельзя также не упомянуть самое очевидное правило – не сообщать посторонним лицам пароли, секретные коды и т.д. Такая проблема возникает, когда мошенники представляются пользователям сотрудниками банка или службой поддержки сервиса.

Таким образом, в данный момент, облачная ЭЦП – это будущее электронного документооборота. Тем не менее, в настоящее время в России еще

не произошло необходимых правовых изменений, которые могли бы защитить владельца облачной ЭЦП.

В заключении, мы можем составить таблицу, где наглядно представим виды угроз и методы защиты в облачной электронной подписи.

Таблица 2 – Меры безопасности при использовании облачной электронной подписи

<table>
<tr><th rowspan="2">Угроза информа-ционной безопасности</th><th rowspan="2">Нарушение информационной безопасности</th><th colspan="2">Виды защиты</th></tr>
<tr><th>Техническая</th><th>Организационная</th></tr>
<tr><td rowspan="6">Угроза конфиден-циальности</td><td rowspan="4">Несанкционированный доступ к информации</td><td>Аутентификация пользователей</td><td>Настройки безопасности в браузере</td></tr>
<tr><td>Защита информации при передаче по каналам связи</td><td>Ограничения на использование сторонних приложений</td></tr>
<tr><td>Контроль доступа</td><td>Установка антивирусного программного обеспечения</td></tr>
<tr><td>Системы обнаружения и предотвращения вторжений</td><td>Использование прошивки от официального производителя</td></tr>
<tr><td>Разглашение информации</td><td rowspan="2">Аналитические системы по выявлению инцидентов информационной безопасности</td><td rowspan="2">-</td></tr>
<tr><td>Утечка информации</td></tr>
<tr><td>Угроза целостности</td><td>Несанкционированное воздействие на информацию</td><td>Средства разграничения и контроля доступа к информации</td><td>-</td></tr>
<tr><td rowspan="2"></td><td>Преднамеренное воздействие на информацию</td><td rowspan="2">Средства разграничения и контроля доступа к информации</td><td>-</td></tr>
<tr><td>Преднамеренное воздействие на информацию</td><td>-</td></tr>
</table>

| **Угроза информационной безопасности** | **Нарушение информационной безопасности** | **Виды защиты** | |
|---|---|---|---|
| | | **Техническая** | **Организационная** |
| Угроза доступности | Несанкционированное воздействие на облако | Системы обнаружения и предотвращения вторжений | - |
| | Преднамеренное воздействие на облако | | - |

Таким образом, мы рассмотрели понятие облачной подписи, выявили её основные недостатки и преимущества, а также разработали меры предосторожности для пользователей таких подписей.

Облачная электронная подпись – современная инновация электронной подписи, которая совсем недавно стала использоваться в России. Учитывая западные тенденции, в нашей стране также возможно её повсеместное использование. Решение по государственному регулированию таких подписей в настоящее время находится только на этапе рассмотрении. Не поставлена также точка во многих вопросах, касающихся безопасности использования облачной подписи.

## 2.4. Защита данных в облачной системе электронного документооборота DirectumRX

Компания Directum – ведущий российский разработчик программного обеспечения в сфере электронного документооборота, занимающийся внедрением систем электронного документооборота (СЭД) в организации с 2003 года по настоящее время, занимает лидирующие позиции на российском ECM-рынке. Цель компании – оптимизация документооборота и внедрение современных технологий в СЭД для повышения эффективности работы предприятий.

На основе облачных технологий сегодня успешно функционирует продукт компании Directum – система электронного документооборота DirectumRX, которая была создана в 2015 году. Система функционирует по принципу модели SaaS (программное обеспечение как услуга) и рассчитана на средние предприятия в количестве 50-200 человек.

В функционал DirectumRX входят такие опции как управление документами, поисковая система, архив документов, ведение договоров, отправка поручений, автоматизированные взаимодействие (т.е. сотрудники могут обмениваться файлами, вести деловую переписку с помощью системы), функция замещения отсутствующего работника.

Данные в DirectumRX хранятся с помощью комбинированного метода – и с помощью SQL-сервера и непосредственно в файлах. То есть, документы, которые используются достаточно редко хранятся в файловом хранилище, а те, что используются постоянно – располагаются в базе данных SQL-сервера. При этом пользователь может работать с этими документами в одной среде. Благодаря такому подходу – использованию разных типов хранения, снижается риск выхода из строя всей системы при сбоях.

Рассмотрим некоторые особенности функционала облачной системы электронного документооборота DirectumRX:

1. В системе есть функция автоматического создания документа по шаблону, который можно настроить.

2. Архив автоматически сортируется по степени актуальности документов.

3. В системе можно использовать любые программы для создания и редактирования документов.

4. Быстрый поиск документов по критериям, например, по реквизитам или самому содержанию документа.

5. В системе ведется история работы с документом.

6. Все данные расположены в одной информационной среде.

7. В систему встроены возможности обмена документами с контрагентами, например, с системой Диадок.

8. В системе используются электронные подписи.

Рассмотрим какие проблемы могут возникнуть в системе безопасности и приведем соответствующие им методы защиты от этих угроз, которые используются в сервисе DirectumRX:

1. Атака на ошибки системы электронного документооборота.

В системе используется регулярный мониторинг всех ошибок, возникающих у клиента в системе. Ошибки проходят сортировку и немедленно устраняются до того, как злоумышленники могли бы воспользоваться ими.

2. Перехват трафика между сервером и клиентским приложением.

Система использует шифрование трафика на основе протокола HTTPS, что защищает, например, от таких угроз как «атака посредника», «перехват пакетов» и др. Даже если взломщик сможет расшифровать данные, то выясниться, что они зашифрованы дополнительно.

Кроме того, в система DirectumRX позволяет проходить аутентификацию и авторизацию на сервере приложений. То есть, если клиентское приложение станет доступно сторонним лицам, то через него нельзя будет получить произвольные данные с сервера, так как проводится дополнительная проверка прав доступа.

3. Атака на ошибки общесистемного программного обеспечения сервера (Вирусы, DDoS-Атаки и др.)

Защиту от подобных атак в DirectumRX осуществляет дата-центр и несет материальную ответственность в случае своих ошибок. Стоит также упомянуть, что между провайдером и клиентом в DirectumRX заключается SLA (Service Level Agreement). SLA – это документ соглашение об уровне обслуживания, где описываются параметры предоставляемых услуг. В случае его нарушения, провайдер должен возместить все убытки от простоев.

4. Получение физического доступа к серверному оборудованию, т.е. самой технике, на которой расположена система.

Данные физически хранятся в дата-центре организации. Внутри этого здания находится охрана, ведется постоянное видеонаблюдение,

контролируются любой доступ. То есть, предприняты все необходимые меры для ограничения попадания посторонних людей к этому оборудованию.

Таким образом, в системе электронного документооборота DirectumRX используются все передовые технологии защиты данных – шифрование информации, аутентификация, использование электронной подписи, мониторинг ошибок, а также сам дата-центр физически защищен и находится под охраной круглосуточно.

Подводя итоги главы, мы можем сделать вывод, что безопасность облачных технологий работы с документами – вопрос в наше время очень актуальный и одновременно спорный.

К вопросу выбора облачных технологий и провайдера для хранения своих документов нужно подходить ответственно. Один из главных шагов, которые должна сделать организация для повышения безопасности своих облачных систем хранения документов – это разработка плана внедрения. Особое внимание стоит уделить способам аварийного восстановления системы, обновлению и исправлений ошибок в работе системы, обязательно проводить тестирование на проникновение угроз.

# 3. МЕТОДИЧЕСКАЯ РАЗРАБОТКА

21 век – век информационных технологий. На сегодняшний день, одно из самых важных знаний для специалиста по работе с документами – это умение ориентироваться в современных технологиях документооборота. Прогресс не стоит на месте, с каждым новым днем появляются все новые способы работы с документами.

Один из таких современных способов – это облачная система работы с электронными документами. Для того, чтобы быть продвинутым специалистом в своем деле, идти в ногу со временем, необходимо разбираться в таких системах, различать их функциональные особенности, учитывать их преимущества и недостатки. Также актуален вопрос безопасности информации в облачных системах документооборота. Необходимо ориентироваться в методах защиты информации, а также знать какие меры предосторожности в них используют.

В разделе представлен конспект лекционного занятия на тему «Облачные технологии работы с документами». Лекционное занятие представляет собой последовательное изложение материала посредством монолога теоретического характера.

Тема занятия – «Облачные технологии работы с документами».

Цель занятия: Ознакомить студентов с основным материалом по теме «Облачные технологии работы с документами».

Поставлены следующие учебно-воспитательные задачи:

1. Обучающая: познакомить студентов с новым материалом.

2. Развивающая: способствовать формированию мыслительных умений: анализа, формулирования понятий, конспектирования.

3. Воспитательная: формирование познавательного интереса, мотивации к обучению с помощью использования наглядных технических устройств.

Оборудование, наглядные пособия: мультимедийное оборудование, компьютер, программное обеспечение: презентация PowerPoint.

При подаче материала учитывались следующие дидактические принципы: принцип научности (теоретические знания по данной теме); принцип систематичности и последовательности (изложение материала в определенной логичной последовательности); принцип наглядности (демонстрация презентации и учебного видеоролика).

Использовались следующие методы изложения материала: рассказ, беседа, иллюстрирование и демонстрация.

Таблица 1 – Структура лекции

| № | Этапы лекционного занятия | Время |
|---|---|---|
| 1 | Организационная часть занятия | 3 мин. |
| 2 | Подготовка к изучению нового материала | 7 мин. |
| 3 | Ознакомление с новым материалом | 40 мин |
| 4 | Закрепление полученных знаний | 35 мин |
| 5 | Рефлексия | 5 мин. |
| 6 | Информирование о домашнем задании | 5 мин. |

Таблица 1. – Ход занятия.

| Ход занятия | Преподаватель | Обучающиеся |
|---|---|---|
| 1. Организационная часть занятия | Приветствует студентов и проверяет готовность к занятию, объявляет тему занятия. | Приветствуют преподавателя и демонстрируют готовность к занятию. |
| 2. Подготовка к изучению нового материала | Актуализация знаний. Сегодня мы рассмотрим современный метод работы с электронными документами – облачные технологии. Вопросы к аудитории: «Перечислите современные технологии, применяемые в настоящее время в электронном документообороте».<br>Тема занятия: «Облачные технологии работы с документами».<br>Пункты плана занятия:<br>1. Понятие облачных технологий<br>2. Виды облачных технологий<br>3. Преимущества использования облачных технологий работы с документами | Отвечают на вопросы преподавателя.<br><br>Записывают тему занятия. |

| Ход занятия | Преподаватель | Обучающиеся |
|---|---|---|
| | 4. Недостатки использования облачных технологий работы с документами.<br>5. Методы защиты информации в облачных технологиях работы с документами | |
| 3. Изучение нового материала | Чтение лекционного материала.<br>1. Понятие облачных технологий<br>На сегодняшний день сложно представить систему управления электронными документами без использования информационно-компьютерных технологий,<br>которые необходимы для увеличения скорости документооборота, повышения мобильности и надежности хранения. В настоящее время все больше предприятий используют так называемые «облачные» системы электронного документооборота.<br>Запишем понятие облачной технологии:<br>Облачная технология - это технология обработки данных, при которой масштабируемые информационные ресурсы и мощности, предоставляются пользователям в качестве услуги через Интернет-соединение.<br>Облачная технология имеет следующие признаки:<br>1. Самообслуживание по требованию. (пользователь вправе выбирать услуги).<br>2. Универсальный доступ по сети (доступ с любого устройства и с любого места через Интернет).<br>3. Объединение ресурсов. (данные хранятся на общих серверах вместе с другими пользователями).<br>4. Эластичность. (пользователь в любое время может изменить предоставляемые услуги). | Слушают.<br><br>Конспектируют. |

| Ход занятия | Преподаватель | Обучающиеся |
|---|---|---|
| | 5. Учёт потребления. (т.е. измеримость услуг).<br>2. Виды облачных технологий. Облачные технологии делятся по моделям обслуживания на IaaS, PaaS и SaaS. Запишем это.<br>IaaS (инфраструктура как услуга) – компьютерная инфраструктура, представляемая в аренду.<br>PaaS (платформа как услуга) – интегрированная платформа для разработки, тестирования и поддержки веб-приложений. Представляется как сервис на основе концепции облачного хостинга.<br>SaaS (Программное обеспечение как услуга) – модель, где пользователю предоставляется программное обеспечение. Разработку и поддержку осуществляет поставщик программного обеспечения.<br>Облачные технологии в зависимости от моделей развертывания делятся на общедоступные, частные и гибридные. Запишем это.<br>Общедоступные облака – находятся за пределами корпоративной сети. Такие сервисы используют множество клиентов и их данные хранятся вместе на одной платформе. Самое легкое и быстрое решение для реализации, но наименее безопасное.<br>Частные облака – разрабатывается для организации, установкой и поддержкой занимается сам клиент. Обеспечивает наиболее сильный контроль и безопасность, в отличии от общедоступного облака.<br>Гибридные облака – смесь общедоступного и частного облака.<br>Клиент сам принимает решение какие операции будут реализованы с помощью общедоступного облака, а какие – с помощью частного. | Конспектируют.<br><br>Конспектируют. |

| Ход занятия | Преподаватель | Обучающиеся |
|---|---|---|
| | Это облако самое сложное для реализации, однако, наиболее выгодное.<br>4. Преимущества использования облачных технологий работы с документами:<br>Преимуществами облачных технологий для работы с документами можно назвать – доступность и мобильность, расширение сотрудничества, удобство использования, экономичность, высокую технологичность, контроль качества, автоматическое обновление программного обеспечения, а также надежность и безопасность данных. Тем не менее, последнее преимущество остается достаточно спорным.<br>5. Недостатки использования облачных технологий работы с документами<br>Можно выделить следующие недостатки облачных технологий - зависимость клиента от Интернет-соединения, технические неполадки и сбои в системе, отсутствие контроля за данными, пожизненные расходы, ограниченную пропускную способность, киберпреступность и вероятность потери данных.<br>6. Методы защиты информации в облачных технологиях работы с документами.<br>Как вы думаете, с какими проблемами безопасности сталкиваются пользователи облачных систем работы с документами и каковы причины этих проблем?<br>Виды облачных угроз можно разделить на четыре типа. Запишем эти типы:<br>1. Традиционные атаки на | Слушают.<br><br>Слушают.<br><br>Отвечают на вопрос.<br><br>Конспектируют. |

| Ход занятия | Преподаватель | Обучающиеся |
|---|---|---|
| | программное обеспечение.<br>2. Функциональные атака на элементы облака.<br>3. Атаки на клиента.<br>4. Атаки на средства виртуализации.<br>5. Комплексные угрозы облачных сервисов.<br>Облачная архитектура безопасности эффективна только при наличии надежных методов защиты.<br>Можно выделить следующие методы защиты облачных систем хранения электронных документов. Запишем эти методы:<br>1. Шифрование данных.<br>2. Защита данных при передаче.<br>3. Аутентификация.<br>4. Изоляция пользователя.<br>7. Электронная подпись.<br>На этом лекционная часть занятия завершена. Давайте перейдем к просмотру презентации и учебного видеоролика. | Конспектируют. |
| 4. Закрепление полученных знаний. | Демонстрирует презентацию, где структурирован и наглядно показан пройденный материал лекции. Далее демонстрирует учебный видеоролик, который посвящен проблемам защиты информации в облачных системах работы с электронными документами. | Смотрят презентацию и учебный видеоролик. |
| 5. Рефлексия | Спрашивает у обучающихся понравилось ли им занятие, выясняет какие недостатки были при проведении занятия и как можно было бы его улучшить. Спрашивает о том, какие выводы они могут сделать к концу занятия | Отвечают на вопросы преподавателя. Делятся эмоциями. Формируют выводы. |
| 6. Информирование о домашнем задании | Озвучивает домашнее задание: каждому из обучающихся подготовить доклад на тему какой-либо существующей облачной | Записывают домашнее задание. |

| Ход занятия | Преподаватель | Обучающиеся |
|---|---|---|
| | системы электронного документооборота | |

Таким образом, по ходу лекции, обучающиеся получили информацию о понятии и видах облачных технологий, их преимуществах и недостатках использования, проблемах безопасности данных в облачных технологиях, а также методах защиты информации в облачных системах работы с документами.

По ходу занятия преподаватель обращает внимание все ли обучающиеся слушали лекцию. Обучающиеся, которые внимательно слушали, а также конспектировали материал, усвоили тему лучше. Применение презентации было направлено на визуализацию лекционного материала, что способствует лучшему запоминанию темы. Учебный видеоролик демонстрировался для того, чтобы закрепить полученные знания.

# ЗАКЛЮЧЕНИЕ

Таким образом, облачные вычисления – современный и перспективный способ работы с электронными документами, который активно развивается как за рубежом, так и в нашей стране.

В данной работе мы рассмотрели понятие облачных технологий, их преимущества и недостатки. Рассмотрели проблемы безопасности в облачных сервисах работы с документами, проанализировали методы защиты информации, подробно изучили применение облачных технологий в электронной подписи, рассмотрели защиту информации в облачной системе электронного документооборота DirectumRX.

Облака представляют множество уникальных преимуществ для работы документами. Это касается в основном их высокой гибкости, мобильности, возможности совместной работы, а также доступности с любого устройства и практически с любой точки планеты.

Облачные технологии работы с документами являются оптимальным решением для работников, деятельность которых связана с постоянным движением – сменой рабочего места, командировками, переездами.

Облачные технологии используются предприятиями и организациями для оптимизации своего документооборота, что способствует повышению производительности бизнеса. Не отстают в этом плане и государственные учреждения.

Особенности облачных технологий, которые подвергаются постоянной критике – это то, что данные хранятся у стороннего поставщика, а также то, что доступ к ним осуществляется только через Сеть. Это означает, что контроль над этими данными ограничен, а также пользователь становиться зависимым от Интернет-соединения. Поднимается вопрос о том, какому провайдеру доверять и каким образом должна быть обеспечена защита.

Основные требования, которые предъявляются сейчас к облачным системам – это обеспечение максимальной беспрерывности соединения, наличие специальных сертификатов и лицензий у компаний, предоставляющих такие услуги, а также гарантии полной безопасности облачных сред.

Безопасность облачных систем невозможна без использования профессиональных методов по защите данных – электронной подписи документа, шифрования информации, мониторинга угроз, аутентификации и идентификации пользователя, мониторинга угроз и прочих методов и программ защиты информации.

В нашем исследовании мы разработали рекомендации для пользователей таких систем, которых стоит придерживаться, чтобы повысить безопасность своего документооборота.

Помимо применения инновационных методов защиты, также очень важно учитывать человеческий фактор. Нужно, чтобы каждый участник процесса понимал свою роль системе защиты данных, поскольку обеспечение безопасности облачной системы хранения электронных документов – это совместная работа провайдера и пользователя.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники:

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_-doc_LAW_61798/

3. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/

4. О бухгалтерском учете: Федеральный закон от 06.12.2011 №149-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW__122855

5. ГОСТ Р 7.0.95-2015. Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200128317

6. ГОСТ Р ИСО 15489-1-2007. СИБИД. Управление документами. Общие требования [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200049980

7. ГОСТ 2.051-2006. ЕСКД. Электронные документы. Общие положения [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200045526

8. ГОСТ Р 50922-96. Защита информации. Основные термины и определения [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006

Литература:

1. Александров К.С. Счет на петабайты // Машины и механизмы. 2013. № 6. С. 20-27.

2. Мурзин Ф.А., Батура Т.В., Семич Д.Ф. Облачные технологии: основные понятия, задачи и тенденции развития // Программные продукты, системы и алгоритмы. 2014. № 1. С. 2-22.

3. Берхольц К.А. Применение облачных технологий в электронном документообороте коммерческих организаций // Инновационное развитие. – 2018. № 10. С. 9-12.

4. Гладкий М.В. Безопасность приложений на платформах облачных вычислений // Труды БГТУ. 2015. № 9. С 204-207.

5. Горохов С.Н, Лобанов Е.М. Современные технологии хранения электронных документов // Вестник архивиста. 2015. № 1. С. 193-200.

6. Гусеев А.В. Перспективы облачных вычислений и информатизация учреждений здравоохранения // Медицинские информационные системы. 2011. № 2. С. 6-16.

7. Денисов Д.В. Перспективы развития облачных вычислений // Прикладная информатика. 2009. № 5. С. 52-58.

8. Довгаль В.А. Облачные вычисления и анализ вопросов информационной безопасности в облаке // Вестник Адыгейского государственного университета. 2015. № 2. С. 160-166.

9. Догваль. Е.М. Методы повышения безопасности в сфере «облачных» технологий // Вестник АГУ. 2014. №4. С. 170-174.

10. Ивонин П.В. Безопасность облака в деталях // Известия ЮФУ. 2013. № 2. С. 35-40.

11. Кодлов П.А. Проблемы безопасности облачных вычислений // Наука, техника и образование. 2016. № 12. С. 54-58.

12. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. № 6. С. 30-34.

13. Лященко Ю.В. Преимущества и недостатки облачных технологий // Актуальные проблемы авиации и космонавтики. 2014. № 8. С.380-386.

14. Максимов Н.В., Алешин Л. И. Информационные технологии: учебное пособие. Москва: Московский международный институт эконометрики, информатики, финансов и права. 2004. 561 с.

15. Малков В.В. Защита информации в облаках для предпринимательского сектора // Вестник Московского государственного университета печати. № 15. 2015. С. 87-93.

16. Овчинников С.А. Облачные технологии как фактор политического риска электронного государственного управления // Автоматика. Вычислительная техника. 2012. № 4. С. 186-190.

17. Растамханова С. Н., Фазлетдинова А. Р., Хафизова Р. Р. «Облачное хранилище данных» в документоведческом аспекте // Молодой ученый. 2016. № 26. С. 81-83.

18. Саломаха Н.А. Угрозы информационной безопасности при использовании облачных электронных подписей // Безопасность информационной среды. 2017. № 14. С. 215-120.

19. Сударкина Е.С. Облачные технологии в госсекторе: преимущества и проблемы внедрения // Электронный вестник Ростовского социально-экономического института. 2015. № 4. С. 20-18.

20. Суханов В.И. Облачный сервис хранения данных // Научный журнал КубГАУ. 2013. № 86. С. 18-33.

21. Хажиева А.С. Принципы защиты информации в облаке // Информационная безопасность. 2016. № 9. С. 7-15.

22. Царегородцев А.В., Савельев И.А., Романовский С.В. Обеспечение безопасности данных в облачных средах // Экономика и управление. 2013. № 4. – С. 68-73.

23. Читчян Р. К. Оптимизация документооборота на предприятии при помощи облачных технологий и перспективы их развития // Научно-исследовательские публикации. 2016. № 2. С. 26-36.

24. Широкова Е. А. Облачные технологии // Современные тенденции технических наук. 2011. № 14. С. 30-33.

25. Шпарло. Е.В. Возможности облачных технологий для хранения документов: за и против // Современный документооборот. 2015. № 7. С. 212-218.

26. Gupta P. The usage and adoption of cloud computing by small and medium businesses // International Journal of Information Management. 2013. № 14. P. 86-82.

27. Mell P., Grance T. The NIST Definition of Cloud Computing (Draft) // Recommendations of the National Institute of Standards and Technology. 2011. № 21. P. 145-208.