Приветствую вас, о, мои драгоценные студенты!

Д/З смотрите в конце лекции!!!
Срок сдачи 5 декабря 2023 года

Данная информация для справки

1 Понятие облачного хранилища данных

Облачное хранилище данных-модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. В противовес модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся, а равно и обрабатываются, в так называемом облаке, которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут располагаться удалённо друг от друга географически, вплоть до расположения на разных континентах.

Другими словами, это своеобразный онлайн-сервис, предоставляющий возможность хранить файлы на удаленном сервере. То есть пользователь может загрузить документ в любое онлайн-хранилище и в будущем использовать его прямо из сервера. С точки зрения клиента, все операции происходят в одном месте, так называемом «облаке». Однако на самом деле, удаленный сервер чаще всего располагается в разных местах, а иногда и на разных континентах. Но это нисколько не затрудняет работу облачных сервисов, так как скорость работы зависит от клиента. А точнее, от скорости Интернет-соединения у клиента, которая желательно не должна быть ниже 600 Кбит/с. Именно поэтому облачные сервисы появились совсем не давно по причине того, что высокоскоростной интернет с предоставляемой скоростью не менее 1 Мб/с. появился в нашей стране.

2 Обзор облачных хранилищ

Облачных хранилищ довольно много, и все они предоставляют различные возможности. Они бывают: платными и бесплатные, рассчитаны на большой объем информации и на малый объем, поддержку разных операционных систем т.д. Единственное, в чем сходны между собой, - в способе обработки информации.

В данном разделе рассматривается одни из самых популярных облачных хранилищ. Такие как:

1. **Dropbox**

Dropbox — облачное хранилище данных, позволяющее пользователям хранить свои данные на серверах в *облаке* и разделять их с другими пользователями в интернете. Его работа построена на синхронизации данных.

Приложение Dropbox можно скачать и инсталлировать на ПК, Mac, Linux или мобильное устройство. Одно из главных преимуществ Dropbox — легкость и интуитив-

ность в использовании — нужно просто закачать файлы в папку Dropbox, опубликовать её, или синхронизировать с нужным устройством. В отличие от основных конкурентов, при работе с Dropbox редактированные файлы не копируются полностью на сервер — осуществляется передача только измененной части информации, предварительно сжатой. Считается, что именно этот факт во многом объясняет известную оперативность работы с Dropbox, по сравнению с аналогами.

Dropbox позволяет пользователю размещать файлы на удаленных серверах при помощи клиента или с использованием веб-интерфейса через браузер. Хотя главный акцент технологии делается на синхронизации и обмене информацией, сервис ведёт историю загрузок, чтобы после удаления файлов с сервера была возможность восстановить данные. Также ведётся история изменения файлов, которая доступна на период последних 30 дней, кроме этого доступна функция бессрочной истории изменения файлов «Pack-Rat».

Главным недостатком Dropbox можно считать подход к выбору папок для синхронизации. Фактически приложение следит за содержимым только одной папки — Dropbox.

Кроме того, в июле 2014 г. в интервью изданию The Guardian известный Эдвард Сноуден сделал заявление, которое может существенно пошатнуть доверие к Dropbox. В частности, он сказал, что Dropbox не в полной мере заботится о конфиденциальности данных пользователя и даже напрямую участвует в глобальной системе слежке PRISM.

PRISM — государственная программа США — комплекс мероприятий, осуществляемых с целью массового негласного сбора информации, передаваемой по сетям электросвязи, принятая американским Агентством национальной безопасности (АНБ) в 2007 году в качестве замены Terrorist Surveillance Program, формально классифицированная как совершенно секретная. (Википедия)

Однако, не все специалисты по безопасности согласны с таким заявлением. Кроме того, использование Dropbox в связке с BoxCryptor, который надежно шифрует файлы перед синхронизацией их с облаком, обеспечивает конфидициальность данных в Dropbox.

Еще один немаловажный недостаток — это то, что дополнительные гигабайты на Dropbox, как правило, имеют срок годности.

2. **Google Drive**

Google Drive — бесплатное облачное хранилище данных, позволяющее пользователям хранить свои данные на серверах в *облаке* и делиться ими с другими пользователями в интернете. После активации заменяет собой Google Docs. В новом сервисе можно хранить не только документы, но и фотографии, музыку, видео и многие другие файлы – всего 30 типов. Но вообще все очень удобно и привычно для пользователей Google-сервисов.

Кроме доступа к сервису через веб-интерфейс, есть возможность доступа через клиенты для Windows, Mac OS и Android, iOS.

3. **Mega**

Mega — (*MEGA Encrypted Global Access*) — это амбициозный новичек, облачный файлообменник Ким Доткома (*Kim Dotcom*), основателя легендарного Megaupload.

Особенностью Mega является то, что сервис шифрует весь контент прямо в браузере с помощью алгоритма AES; пользователи могут передавать друг другу файлы в зашифрованном виде, при этом все данные хранятся в «облаке»; ключи доступа к файлам не публикуются в открытом доступе, а распространяются по схеме Friend-to-Friend, между доверяющими друг другу пользователями.

По предоставляемому дисковому пространству и по его стоимости, Mega, несомненно можно назвать одним из самых выгодных облачных сервисов, кроме того, важное отличие Mega от других подобных сервисов — конфиденциальность, ведь Mega позиционируется как сервис, который защищает личные данные пользователя. Однако, есть пока и недоработки, в частности, Mega пока проигрывает другим флагманам облачных хранилищ данных в синхронизации с разными устройствами.

4. **Яндекс.Диск**

Яндекс.Диск — бесплатный облачный сервис от Яндекса, позволяющий пользователям хранить свои данные на серверах в облаке и передавать их другим пользователям в интернете. Работа построена на синхронизации данных между различными устройствами. В настоящее время регистрация пользователей доступна всем. Ранее, до запуска Яндекс. Диска, функции хранения пользовательских файлов на Яндексе выполнял сервис Яндекс.Народ.

Кроме того, Яндекс.Диск может выступать в качестве службы облачного сервиса, интегрируясь в офисный пакет Microsoft Office 2013, а недавно появилась возможность автоматической загрузки фото и видеофайлов с цифровых камер и внешних носителей информации на Яндекс. Диск.

5. **Copy.com**

Copy.com — новый конкурент Dropbox, перспективный «новичек» среди облачных хранилищ данных. По функционалу практически идентичен Dropbox. Разработчик данного сервиса — компания Barracuda Networks, деятельность которой является защита данных, анонсируется хорошая безопасность и защита данных.

Из плюсов Copy.com можно отметить красивый и понятный интерфейс; кроссплатформенность сервиса — есть приложения для Android, iOS, Linux, Mac OS X, Windows и Windows Phone; отсутствие ограничения на размер загружаемого файла.

3 Безопасность хранения данных в облаке

Google Drive

Веб-гигант Google предоставляет множество прекрасных функций в своем облачном хранилище. Google говорит, что хранить данные у них безопасно. Даже если ваш

компьютер, планшет или телефон выходят из строя, данные на Google Drive находятся в безопасности. Компания также утверждает, что файлы, хранящиеся у них в дата-центре, не могут исчезнуть.

Чтобы использовать Drive, вам необходима учетная запись Google. Создать учетную запись в Google проще простого. Google предложит вам придумать надежный пароль. Пароль должен содержать как минимум 8 символов. Тем не менее, требования к чувствительным к регистру или разнообразным буквам и числам при регистрации в Google отсутствуют. Хотя это могло бы улучшить безопасность.

Защита учетной записи в Google — это основной шаг по обеспечению безопасности в хранилище Drive. Google предлагает двухшаговую верификацию(двухфакторную аутентификацию) для того, чтобы увеличить надежность учетной записи. Как только вы активируете эту функцию, при каждом входе в какой-либо из сервисов Google вам нужно будет вводить дополнительный код. После ввода правильного имени пользователя и пароля на странице учетной записи в Google вы получите СМС с кодом верификации на свой мобильный телефон. Вы сможете войти в Google только после ввода этого кода. Таким образом, двухшаговая аутентификация может сделать Google Drive более защищенным от хакеров. Вы также можете получать такие коды с помощью приложений для смартфона.

В учетной записи Google есть секретный вопрос и возможность ввода электронного адреса или номера телефона для восстановления учетной записи, а также это позволить возобновить контроль над учетной записью в случае взлома. Вы также контролируете приложения, в которые вы входите с помощью своей учетной записи. Также доступны журнал посещений, IP-адрес и данные об устройстве, чтобы вы могли отслеживать активность по своей учетной записи Google.

Шифрование просто жизненно необходимо для любого облачного сервиса. Несмотря на то, что Google Drive в работе использует HTTPS, он не предоставляет собственную услугу по шифрованию файлов. Так что если вы хотите зашифровать файлы, сделайте это до отправки их на Google Drive. Вы можете бесплатно воспользоваться программой Boxcryptor, чтобы обезопасить свои облачные файлы.

Google Drive предлагает целый ряд индивидуальных опций для обмена. Используя эти настройки, вы можете определить, кто может иметь доступ к файлам, кто может их загружать, редактировать и т. д. Вы можете просматривать версии файловна Google Drive. Так что если вам необходима предыдущая версия, вы можете ее получить, нажав на правую кнопку мыши на необходимом файле и выбрав опцию ‘Управление версиями’.

Можно отметить, что безопасность сервиса онлайн-хранения данных от Google зависит от безопасности учетной записи Google. Если можно защищать свои учетные записи Gmail ID, тогда смело можно рассчитывать на надежную защиту файлов на Google Drive.

Microsoft OneDrive

Облачное хранилище OneDriveот мощнейшего разработчика софта Microsoft. Для того чтобы использовать OneDrive, необходимо обзавестись учетной записью

Microsoft. ПосетитеOutlook.com, чтобы открыть новую учетную запись Microsoft. Во время подписки Microsoft принимает ряд надежных мер безопасности, чтобы защитить потребителя от действий хакеров. Microsoft предлагает и требует ввода сложного пароля, состоящего минимум из 8 символов с регистрочувствительными буквами. Все это делается ради безопасности.

Безопасность OneDrive зависит от безопасности учетной записи Microsoft. Поэтому, если учетная запись Microsoft защищена, это также поддерживает безопасность пространства на OneDrive.

Microsoft подходит очень серьезно к вопросам безопасности учетных записей на Outlook.com. Для создания учетной записи нужно зайти в опцию «Настройки учетной записи», там подтвердить свою личность, используя двухшаговую аутентификацию. Для настроек учетной записи эта функция включена по умолчанию.

Двухшаговая верификация Microsoft обладает большим функционалом, чем аналогичная функция от Google. Тем не менее, можно спокойно доверять обоим сервисам.

В своей работе OneDrive использует соединение HTTPS. ‘Недавняя активность’. Оттуда также можно управлять приложениями, использование которых разрешили вместе с Outlook.com.

OneDrive предлагает функцию бесплатного просмотра истории файловдля офисных документов. ‘Предыдущие версии’ других форматов файлов доступны для пользователей бизнес-уровня. Поэтому, если вносить изменения в документы Office, в OneDrive можно бесплатно просмотреть их предыдущую версию. Файлы OneDrive недоступны без вашего на то разрешения. Несмотря на это, OneDrivene шифруетзагружаемые на его сервер файлы. Таким образом, можно обеспечить более высокий уровень безопасности для своих данных, можно воспользоваться сторонними сервисами для шифрования, например,Boxcryptor.

Dropbox

Dropbox — это один из самых популярных провайдеров онлайн-хранения данных. Его используют как в личных, так и в коммерческих целях. Dropbox— это исключительно облачное хранилище. Так что все их силы сконцентрированы на облаке..

Dropbox говорит, что безопасность данных — это их первоочередный приоритет. При подписке на Dropbox можно заметить, что этот процесс довольно простой и быстрый. Потребуется ввести имя, адрес электронной почты и пароль. Страница создания учетной записи предложит использовать надежный пароль. Тем не менее, обязательства относительно поддержания определенного уровня безопасности отсутствуют.

Подписка на Dropbox может не потребовать немедленной верификации электронного адреса, но для того, чтобы беспрепятственно обмениваться файлами, необходимо подтвердить свою электронную почту. Все эти опции будут доступны по мере использования сервиса.

Dropbox предлагает функцию версии файлов для того, чтобы можно было вернуться к старой версии необходимых файлов. Если файл был отредактирован, а позже понадобилось получить его предыдущий вариант, просто нажать на правую кнопку мыши на новой версии файла, и выберите опцию «Предыдущие версии» в контекстном меню.

Учетная запись Dropbox предоставляется с целым рядом дополнительных систем безопасности. Также можно использовать двухшаговую верификацию, при которой необходим ввод уникального кода при каждом входе в Dropbox. Этот код можно получить на мобильный телефон. Также можете получить код через приложение для смартфонов. В любом случае, двухфакторная аутентификация может существенно увеличить уровень безопасности вашей учетной записи.

На странице настроек безопасности Dropbox также можно мониторить и управлять подсоединенными устройствами, журналом посещений, привязанными приложениями и т. д., с целью предотвращения несанкционированного доступа.

Dropbox использует соединение HTTPS на своем сайте и во время передачи данных между вами и облачным хранилищем. Можно контролировать доступ к файлам с помощью опций обмена данными.

Сам Dropbox не предоставляет опцию шифрования файлов до загрузки на их сервер. В Dropbox уверяют, что они шифруют файлы во время передачи и в течение всего остального времени. Тем не менее, можно зашифровать файлы до отправки на Dropbox. Для этого существует целое множество инструментов.Boxcryptor— один из них. Он использует стандартную технологию шифрования «AES-256 bit», чтобы еще больше увеличить уровень безопасности ваших файлов.

Copy

Copy — один из самых популярных сервисов облачного хранения данных, конкурирующий с Dropbox, Google Drive, OneDrive и т. д. Сервис также предлагает бонус за привлечение новых клиентов, с помощью которого существующие пользователи могут увеличить свое бесплатное пространство. Процесс регистрации на Copy занимает всего несколько секунд. Вас попросят указать имя, адрес электронной почты и пароль. В процессе регистрации на Copy. Все что было указано касательно пароля — он должен состоять как минимум из 6 символов.

Copy.comиспользует безопасное HTTPS соединение во время передачи данных между пользователем и своим сервером. Компания такжеутверждает, что они хранят данные в зашифрованном формате. Но несмотря на это, нельзя самостоятельно шифровать данные на Copy.com. Но никто не отменял сторонние сервисы по шифрованию данных перед их отправкой на Copy. Так что спокойно можно вначале зашифровать файлы, а потом отправить их на хранение в Copy.

Copy.com не предлагает двухшаговой верификации, которая играет очень большую роль в поддержании безопасности учетной записи. Надеюсь, что вскоре они начнут предлагать эту ценную опцию.

В Copy есть функция проверки истории файлов, с помощью которой можно получить предыдущие версии своих файлов. К сожалению, в Copy.com нету опции просмотра истории посещений учетной записи.

Несмотря на прекрасный пользовательский интерфейс и функциональность, Copy все еще не хватает некоторых необходимых функций.

Mega

Сервис Mega, который известен своей конфиденциальностью. Mega был основанKim Dotcom. Сервис предоставляет каждому новому пользователю 50 Гб бесплатного пространства. Для регистрации в Mega необходимо предоставить такую основную информацию, как имя, адрес электронной почты, пароль и т. п. Mega требует использовать надежный пароль. Если пароль недостаточно сложный, вы получите следующее сообщение: ‘ваш пароль недостаточно надежен чтобы продолжить’.

Mega использует HTTPS соединение и технологию шифрования клиентской части. Это значит, что локально зашифрованная информация будет отправлена на Mega. При загрузке информации с сервиса, она расшифровывается. Как утверждается на странице помощи по вопросам безопасностиMega, ваши файлы невозможно читать на сервере. Компания настоятельно рекомендует не терять пароль. Пароль к Mega это не только пароль, а код, который открывает основной ключ дешифровки. Mega утверждает, что пароль на сервисе восстановить невозможно. Если нет резервной копии основного ключа дешифровки то, тогда потеряется и все данные, хранящиеся на сервере сервиса.

Тем не менее, существуют сообщенияо том, что в системе шифрования Mega на базе браузера есть определенные слабости.

Mega предлагает прекрасные средства безопасности, но, к сожалению, истории версий файлов у сервиса нет. Можно восстановить удаленные файлы с помощью приложения ‘SyncDebris’ от Sync Client, или из папки ‘Rubbish Bin’ на Mega. Для мониторинга активности Mega предоставляет опцию журнала посещений и опцию управления приложениями.

Интересно то, что у Mega нет опции двухшаговой верификации, которая могла бы намного улучшить усилия сервиса, касающиеся конфиденциальности и безопасности.

В данном разделе были подробно рассмотрены доступные средства безопасности популярных провайдеров облачного хранения данных, таких как Google Drive, Dropbox, Copy и Mega. Что касается безопасности, у всех у них есть собственные и особые предложения. Теперь посмотрим какие же основные средства безопасности предлагают эти сервисы. Ниже представлен удобный для ознакомления контрольный список.

1. Требование к надежности пароля: Google, Microsoft и Mega требуют использовать надежный пароль. Dropbox и Copy более гибкие в этом плане.
2. Требование верификации адреса электронной почты: Все сервисы рано или поздно требуют верифицировать свой электронный адрес.

3. Двухшаговая верификация: Google Drive, OneDrive и Dropbox предоставляют двухшаговую верификацию. Copy и Mega на данный момент не предоставляют такой опции.
4. Шифрование клиентской части: Только Megaпредлагает шифрования клиентской части. Это осуществляется с устройства, с которого загружаются файлы.
5. Шифрование серверной части: Dropbox, Mega и Copy хранят файлы на серверах в зашифрованном виде. Где можно использовать локальное шифрование, чтобы избежать рисков.
6. Использование безопасного соединения (HTTPS): Все эти провайдеры используют безопасное соединение HTTPS. Тем не менее, Mega дает пользователям выбор его отключить (по выбору).
7. Использование секретных вопросов для верификации пользователей: У Google Drive эта опция доступна. OneDrive, Dropbox, Copy и Mega на данный момент не используют секретный вопрос.

Из вышеуказанного становится ясно, что Google Drive предоставляет почти все средства безопасности, кроме шифрования. Microsoft OneDrive и Dropbox идут следом за ним. Mega предоставляет такое сложное средство безопасности, как шифрование, но на сервисе отсутствует двухшаговая верификация. Copy необходимо поработать над тем, чтобы превратить прекрасное облачное хранилище в более безопасную среду с помощью двухшаговой верификации, требования к надежности пароля и других инновационных систем безопасности.

Заключение

В заключении стоит сказать, что на данный момент идет активная разработка и совершенствование технологии облачных вычислений. Но речь идет именно о разработке, а не об использовании. На данный момент многие бояться именно самого факта, что информацию будут хранить сторонние люди. И хотя почти невозможность утери либо кражи данных уже доказана, немногие готовы довериться подобным сервисам. Так же сказывается недостаточное на данный период времени качество, стабильность и скорость Интернет-соединений, что создает ощутимые трудности для разработчиков.

Однако несмотря на эти существенные недостатки, плюсы от внедрения данной технологии ясны всем. Ведь это экономия для потребителей, борьба с пиратством для разработчиков, минимизация затрат в IT сфере для бизнеса, унификация сетевых стандартов для всех пользователей.

Облачные хранилище данных очень нужны в наше время. В подтверждение этому можно привести ряд причин: нехватка мест на жестком диске, не долговечность ОС, «беготня с флэш картой» и так далее.

Считаю, что поставленные в работе цели и задачи выполнены в полном объеме. В работе указано, что облачные хранилища представляют собой своеобразный онлайн-сервис, предоставляющий возможность хранить файлы на удаленном сервере. Главный плюс то, что имеется доступ к вашим данным с любой точки земного шара, где есть интернет. Главный минус - это безопасность и конфиденциальность при передаче или получении данных.

В работе говорится о самых известных «облаках». Таковыми являются: Dropbox (В частности, в Dropbox нет возможности редактирования документов, зато здесь нет и никаких ограничений на формат и размер мультимедийных файлов), Яндекс. Диск (Он имеет самую большую скорость (2-3 мегабайта в секунду) и возможность подключить диск по WebDav. Это довольно большие плюсы), GoogleDrive(Главными достоинствами Google является невысокая стоимость дополнительных гигабайт и тесная интеграция с Google Docs, позволяющая редактировать файлы онлайн).

В данной работы, решена главная задача: сравнение и выявление по определенным признакам (потребление памяти, потребление памяти, время загрузки файла, доступное место, доступное место после выполнения несложных действий, увеличение доступного пространства за счет инвайтов, максимальный размер файла, Windows, Mac, Android, IOS, Веб-доступ, возможность синхронизации любых папок на диске, возможность редактирования документов онлайн, публичные ссылки на файлы, восстановление предыдущих версий файлов) самое лучшее облачное хранилище.

Список использованных источников

1. Медведев А. Облачные технологии: тенденции развития, примеры исполнения// Современные технологии автоматизации. 2013. № 2. С.6-9.
2. https://ru.wikipedia.org
3. Эталонная архитектура облачных вычислений - Рекомендации Национального Института Стандартов и Технологий (США), NIST, USA, 2007
4. http://softlab.pp.ua/article/333-oblachnye-vychisleniya-vitayut-v-oblakax.html статья «Облачные вычисления витают в облаках»
5. Екатерина Баранова, «Концепция Cloud computing» http://www.itcontent.ru/archives/blog/cloud_computing

10. Основы Облачных вычислений (по рекомендациям NIST) http://cloud.sorlik.ru/synopsis-4.html

11. Черняк Л. Интеграция - основа облака. //Открытые системы. СУБД 16 сентября 2011 г.

http://bourabai.kz/mmt/cloud.htm

Климентьев В.П., Устинов В.А. Введение в облачные вычисления. [Электронный ресурс] – URL:http://lib.convdocs.org/docs/index-63430.html(дата обращения 20.11.2023)

Д.з.

По предложенному материалу создать презентацию.

Д/З прислать на электронную почту:

bengi-oskal@yandex.ru

Адрес скопировать и вставить в строку адресата.

Требования к презентации: Заголовок кегль 48 пунктов, содержание текста: кегль 28 пунктов

1-й слайд - Титульный лист. Обязательно!

Информация на слайде:

Тогучинский политехнический колледж

Тема: «Разновидности компьютерных сетей»

Выполнил: ФИ, группа

Проверил: О.А. Петроченко

2-й слайд – Содержание

Далее по содержанию. Количество слайдов: не менее 10! 2 слайда, можно сказать уже готовы.

Желаю успехов! Надеюсь на сотрудничество!

Берегите себя!