Содержание:

Введение

Термин «облачные вычисления» (cloud computing) стал активно употребляться с 2008 года. Разработчики облачных вычислений определяют их как инновационную технологию, которая предоставляет динамично масштабируемые вычислительные ресурсы и приложения через Интернет в качестве сервиса под управлением поставщика услуг.

Одним из наиболее значимых событий в данной области было появление в 1999 г. компании Salesforce.com, которая стала первой, кто предоставил доступ к своему приложению через сайт. Фактически Salesforce.com впервые предоставила программное обеспечение по принципу «программное обеспечение как услуга» (SaaS – software as a service).

Следующим этапом стало создание в 2002 г. компанией Amazon веб-сервиса, позволяющего хранить данные и производить вычисления. В 2006 г. Amazon запустила веб-сервис, который позволял его пользователям запускать свои собственные приложения. Еще одним важным шагом стало создание компанией Google платформы Google Apps для веб-приложений в бизнес-секторе.

Облачные сервисы принято подразделять на несколько моделей:

Предоставление программного обеспечения как услуги (Software as a service, SaaS) - клиент получает доступ к приложениям, которых находятся в облачной инфраструктуре. Где и на каком оборудовании выполняется приложение, клиент может не знать. Предоставление рабочего места как услуги (Desktop as a service, DaaS) - клиент получает полностью готовое к работе («под ключ») стандартизированное виртуальное рабочее место, которое каждый пользователь имеет возможность дополнительно настраивать под свои задачи. Предоставление платформы как услуги(Platform as a service, PaaS) - Клиент может устанавливать и разрабатывать свои приложения на предоставленной платформе. Клиент контролирует приложения, имеет частичный контроль над платформой, но не контролирует инфраструктуру. Предоставление инфраструктуры как услуги (Infrastructure as a service, IaaS) - Клиенту предоставляется виртуальная архитектура, состоящая из серверов, рабочих станций и сетевого оборудования,

где клиент сам может разворачивать свои собственные операционные системы, базы данных и приложения.

Половина специалистов считает, что облачные технологии в будущем станут основой ИТ-структуры компании. Однако другая половина обеспокоена вопросами безопасной эксплуатации подобных сервисов, потерей контроля и невозможностью использования привычных инструментов. Так согласно опросу проведенного Symantec о виртуализации и переходе в облака за 2011 год, 44% руководителей опасаются перемещать критически важные для бизнеса приложения в облачные среды, причем 76% из них считают вопрос безопасности основной проблемой. Ведь если хакеру все же удастся взломать защиту облачной среды, объемы потерянных данных будут во много раз больше, нежели в результате взлома отдельного компьютера или локальной сети.

Вопрос здесь стоит скорее в привычках. Показательным является тот факт, что облачные среды для хранения информации, активно используют правительственные и военные организации многих стран, в том числе – министерство обороны США, NASA, ЦРУ, ФБР и другие. И вряд ли у них заниженные требования к безопасности.

Сама идея размещения приложений и данных на внешних ресурсах, показывает, что задача обеспечения безопасности имеет совсем другие корни, а поэтому решать их нужно несколько иначе, и при помощи других инструментов. При этом к классическим и типичным для виртуализации проблемам, добавились свои, главная из которых кроется в самом принципе организации данных.

Целью данной работы является познакомиться с понятием «облачные сервисы».

В соответствии с поставленной целью будут решены следующие задачи:

- рассмотрена анатомия облачной инфраструктуры хранения данных;

- приведен алгоритм выбора облачного хранилища данных;

- исследована безопасность хранилища данных в «облаках»;

- проведен сравнительный анализ облачных сервисов.

Курсовая работа состоит из введения, трех глав, заключения и списка литературы.

Глава 1. Анатомия облачной инфраструктуры хранения данных

1.1. Облачные технологии

Прежде чем рассматривать облачные хранилища данных, стоит сначала обратить внимание на технологии, лежащие в их основе, то есть на «облачные технологии». Что же они из себя представляют?

Облачные технологии – это удобная среда для хранения и обработки информации, объединяющая в себе аппаратные средства, лицензионное программное обеспечение, каналы связи, а также техническую поддержку пользователей. Работа в «облаках» направлена на снижение расходов и повышение эффективности работы предприятий. Особенностью облачных технологий является не привязанность к аппаратной платформе и географической территории, а возможность масштабируемости. Клиент может работать с облачными сервисами с любой точки планеты и с любого устройства имеющего доступ в интернет, а также оперативно реагировать на изменяющиеся бизнес-задачи предприятия и потребности рынка.

Таким образом, данный подход к хранению и использованию информации существенно расширяет возможности пользователей.

Практическим воплощением облачных технологий явилось появление облачных хранилищ данных. Благодаря появлению облачных хранилищ, гораздо проще и выгоднее разместить файлы в «облаке» и спокойно менять свое местоположение, зная, что в любой момент к ним есть доступ при наличии канала в Интернет. С помощью «облака» удобно как хранить данные, так и обмениваться информацией с другими людьми. Для этого нужно только отправить ссылку получателю, и он имеет возможность загрузить файлы в подходящий для него момент. Также, чтобы избежать потери нужной информации, достаточно просто скопировать ее в «облако» и периодически обновлять.

Все перечисленные выше причины дают нам возможность понять преимущества облачного хранилища для размещения файлов перед традиционным.

Так что же это такое «облачное хранилище данных»?

Облачное хранилище данных — модель онлайн-хранилища, в котором данные хранятся на многочисленных, распределённых в сети серверах, которые предоставляются 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 и обрабатываются, в так называемом «облаке», которое являет 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.

Облачное хранилище данных – это организация, которая раздаёт всем желающим свободное место на своих серверах (бесплатно, платно или условно–бесплатно).

Эта организация также предоставляет дополнительные услуги для пользователей облачного хранилища, с помощью которых есть возможность получить не только простой доступ к информации с компьютера или мобильного устройства, но и повысить уровень безопасности данных, осуществлять автоматическую синхронизацию данных между компьютерами и устройствами пользователя, а также предоставлять общий или ограниченный доступ к своим файлам.

Чтобы использовать сервис облачного хранилища данных, нужно на все компьютеры или мобильные устройства установить специальную программу–клиент облачного хранилища и указать папки жёсткого диска компьютера, которые нужно поместить в «облако». Эта программа скопирует указанные папки и файлы в «облако» и будет следить за изменениями файлов в этих папках на том компьютере, где она запущена.

Если внести какие–либо изменения в контролируемой папке, то программа автоматически внесет аналогичные изменения в облачное хранилище. Те же самые действия будут происходить и в обратном порядке: если в «облаке» внесены изменения в файлах, а на жёстком диске компьютера их нет, то программа внесёт изменения в файлы компьютера.

Таким образом, если подключить к облачному хранилищу несколько компьютеров или мобильных устройств, на каждом из них будет присутствовать всегда нужный набор файлов. Также появится возможность отредактировать файл на компьютере, а затем открыть его в ноутбуке, и он всегда будет последней, изменённой версией.

Не исключено, что во время автоматической синхронизации данных через облачное хранилище возможны ошибки, которые связаны с работой программного обеспечения или с «человеческим фактором». Чтобы минимизировать проблемы, нужно использовать облачное хранилище данных, которое помнит историю изменения файлов. Также перед тем, как выключить свой компьютер, нужно всегда дожидаться полной синхронизации файлов.

К сожалению, новые данные из «облака» не появляются сразу после включения компьютера, потому что нужно время для синхронизации данных. Поэтому эффективное применение облачных хранилищ предполагает наличие быстрого и безлимитного Интернет на всех компьютерах.

1.2. Примеры облачных сервисов

На сегодняшний день существует более пятидесяти компаний предоставляющие облачные сервисы. В данном пункте работы будет рассмотрены наиболее лучшее решения в сфере облачных технологий и проведено их сравнение.

Azure Cloud Drive

Облачное хранилище от компании Azure – для тех, кто использует Kindle, то это лучший вариант, но по работоспособности он уступает тому же Google Drive. Выделяется бесплатно 5 Гб объема на диске, также существуют приложения для Android и iPhone, и версии для Mac и PC.

Apple iCloud

Для пользователей Apple отличным решением является возможность выполнения резервного копирования всех важных файлов на iOS и Mac устройствах, и затем синхронизировать требуемые данные. Но данное средство создано больше для мобильных устройств, к примеру, загрузка определенного типа файлов не выполнится из-за того, что этот тип файлов ими не поддерживается. Также бесплатно выделяется 5 Гб места, но можно выделить еще место, например 10, 20, и даже 50 Гб. Кроме операционных систем Apple, сервис может поддерживаться на устройствах с ОС Windows.

Ubuntu One

Запущенно создателями компании Canonical - одноименный линукс-дистрибутив Ubuntu. Данный сервис может вполне нормально работать и на устройствах с Windows (с Win 8 не все нормально работает), и на Mac компьютерах. Пользователям бесплатно выделяют 5 Гб пространства на диске (а еще туда встроен сервис потокового онлайн вещания «стриминг» музыки), а за следующие 20 Гб нужно тратить средства или $2.99 за месяц или $29.99 за год. Если пользователь использует Ubuntu, и требуется облачный сервис, то лучшего не найти.

SugarSync

Данное средство используют для резервного копирования данных и их синхронизации. Основные конкуренты SugarSync это Dropbox, Mozy и Box, но сервис не теряется даже в такой ответственной компании, и большим плюсом есть возможность выбрать какие именно папки и файлы загрузить в облако и синхронизировать. Им пользуются бесплатно только 30 дней, затем требуется тратить средства для дальнейшего использования. Начальные тарифы от $74.99 в год за 60 Гб пространства, а максимум можно приобрести 500 Гб, стоимость которых $399 за год.

Google Drive

Бесплатно пользователю предоставляется 15 Гб пространства на диске, а докупленное дополнительно пространство распределяется между всеми сервисами Google - Gmail, Google+ и диском. Кроме 1, 10 и 100 Тб, есть тарифы на 20 Тб - стоимость которых составляют $199.99, и 30 Тб за $299.99.

Dropbox

Удобный сервис, который создан для синхронизации файлов между разными устройствами и компьютерами. Бесплатно пользователю предоставляют 2 Гб дискового пространства (но есть возможность увеличить пространство с помощью разных хитростей и участия в акциях по типу «пригласи друга»), далее следует «расширенный» аккаунт на 100 Гб за $9.99 в месяц, следующий тариф - 500 Гб за $49.99 в месяц (или $499 в год). Следующие тарифы Dropbox созданы для бизнеса - на пять пользователей с безграничным Storage стоимость $15 на пользователя в месяц. Претензий нет к детищу Дрю Хьюстона, но доступ мог бы быть бесплатным к истории изменения файлов (данную функцию называют Packrat).

Box

Это один из самых старых облачных сервисов. Аккаунт рассчитан на 10 Гб бесплатного пространства, с учетом того что объем загружаемых файлов не должен превышать 250 Мб. За $10 пространство на диске можно увеличить до 100 Гб, а следующие тарифы рассчитаны на несколько человек. Box в своей основе создан для корпоративных клиентов, а не для обычных пользователей, о чем свидетельствует существование таких функций как, к примеру, интеграция с Google Apps и Salesforce.

Microsoft OneDrive

Чуть менее раскрученный, но от этого более интересный сервис. Microsoft раскручивал предшественника OneDrive (прошлое название SkyDrive) в течении нескольких лет, и вскоре случилось переоформление сервиса. На данный момент OneDrive интегрирован с Windows 8 и имеет поддержку некоторых новых устройств (также существует приложение для XBox). Функционал этого сервиса довольно большой - синхронизация файлов между разнообразными ПК, возможность редактирования в вебе документов с помощью приложения Office Web Apps. Бесплатно пользователю дается 7 Гб пространства на диске (раньше в SkyDrive предоставляли целых 25 Гб), также есть платные варианты с 50Гб за $25, 100Гб за $50 и 200 Гб за $100.

Mozy

Сервис Mozy раньше сосредотачивался лишь на бэкапе файлов без возможности синхронизации на разных ПК и устройствах, но в будущем данная функция была добавлена. Кроме простоты применения, Mozy не то средство, которое нужно выбрать, когда вы редактируете и делитесь файлами с помощью облака. А использовать данный ресурс стоит когда вы хотите скопировать весь свой диск в случае внезапной катастрофы. Еще есть один минус – это отсутствие бесплатной версии, существуют только платные тарифы - начало от $9.99 за 10 Гб в месяц и заканчиваются 1 Тб за $379.99 (если уплатить за весь год, то будет дешевле).

Bitcasa

Это молодой сервис, который основали бывшие сотрудники Mastercard, VeriSign, Classmates.com и Mozy. За $10 в месяц есть возможность получить неограниченное пространство на диске. Также существует бесплатный тариф, в котором выделяется 10 Гбайт пространства на диске, что тоже достаточно. У Bitcasa стандартный набор приложений и поддерживаемых платформ, кроме этого, существует плагин для Chrome, который еще проще использовать.

Яндекс.Диск

Бесплатно пользователю доступны 10 Гб пространства после подключения Диска, также можно увеличить пространство с помощью «пригласи друга» (предоставляют по половине 1Гб за приглашенного пользователя), принимать участие в акциях и платить средства. Возможность оплаты разная, платить можно помесячно, а можно приобрести место на год вперед, что чуть выгоднее - дополнительные 10 Гб стоимость 300 рублей за год (за месяц - 30), 100 Гб будут стоить 1500 рублей за год (150 рублей за месяц). 1 Тб стоит 9000 рублей за год (900 рублей за месяц).

1.3. Анализ нормативной базы безопасности облачных сервисов

Для управления информационными рисками необходимо выполнять процесс по выявлению и оценки таких рисков, а также понижать до приемлемого уровня безопасности. Для решения задачи по управлению рисками необходимо выявить уязвимости и угрозы, оценить возможное воздействие, позволяющие применить адекватные меры защиты, собственно для систем, которым необходима защита. Такое управление рисками дает возможность сделать безопасность эффективной с экономической точки зрения, актуальной и способной своевременно прореагировать на угрозы. Данный процесс по управлению рисками позволяет поставщику услуг приоритезировать перечень рисков и назначить благоразумную стоимость мер защиты.

Для управления информационными рисками необходимо выполнить 4 основных пункта: идентифицировать угрозы и уязвимости, идентифицировать активы и определить их ценность для поставщика услуг, обеспечить экономический баланс меж ущербом от действия угроз и стоимостью мер защиты, провести количественную оценку вероятности и влияния потенциальных угроз на поставщика услуг.

Чтобы обеспечить процесс управления рисками в настоящий момент применяют различные стандарты, технические регламенты и нормативные документы. ISO/IEC 15408, серия ISO/IEC 27000 представляет собой один из необходимых документов при построении систем защиты информации СЗИ облачных ИТКС.

Международный стандарт ISO/IEC 15408. Российский ГОСТР ИСО/МЭК 15408-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» являет собой перевод международного стандарта ISO/IEC 15408:2005 на русский язык.

Оценивая риски необходимо установить возможность успешной атаки на ИТКС, когда применяется попытка атаки. Этот показатель, несомненно, зависит от эффективности реализации функций безопасности объекта.

В разделе AVA_SOF описана стойкость функции безопасности объекта оценки. Она определяется, как «характеристика функции безопасности объекта оценки, показывающая минимальные усилия ,которые предположительно необходимы для нарушения ее ожидаемого безопасного поведения при прямой атаке на располагающиеся в ее основе механизмы безопасности.

Такое понятие, как «потенциал нападения», применяют при проведении процедуры анализа стойкости функции безопасности объекта оценки и для анализа уязвимостей.

Предполагается три разновидности стойкости функции безопасности- базовая , средняя и высокая.

Стойкость базовая обеспечит адекватную защиту объекта при случайном нарушении его безопасности со стороны нарушителя, который имеет низкий потенциал нападения.

Стойкость средняя обеспечит защиту объекта при целенаправленном нарушении его безопасности со стороны нарушителя, который имеет умеренный потенциал нападения.

Стойкость высокая обеспечит защиту объекта при спланированном и организованном нарушении его безопасности со стороны нарушителя, который имеет высокий потенциал нападения.

Потенциал нападения напрямую зависит от уровня компетенции и мотивации нарушителя, а также от возможностей ресурсов - информационно-телекоммуникационных систем.

При проведении анализа потенциала нападения изучаются нижеперечисленные факторы:

1. При идентификации уязвимости:

- время, которое затрачивается на идентификацию уязвимости ИБ;

- знание проекта и функционирования объекта оценки;

- уровень подготовки;

- программное обеспечение и аппаратные средства,

- доступ к объекту оценки.

При использовании:

- время, израсходованное на использование уязвимости ИБ;

- возможность доступа к объекту оценки

-уровень специальной подготовки;

- знание проекта функционирования ИТКС;

- программное обеспечение, аппаратные средства, обеспечение и другое оборудование, применяемое для использования уязвимости.

Дальше по этим факторам назначают веса, которые суммируются. Эту сумму используют для оценки уязвимости (потенциала нападения и СФБ ОО). С технической точки зрения, ГОСТ 15408 рассматривает полноту СЗИ, не рассмотрев при этом комплекс организационных мер. Заключение о состоянии защищенной ИС нужно проводить на основе состояния защищенности всех ее составляющих, при реализации уязвимостей которых, ИТКС способна прийти в недопустимое состояние.

В серии стандартов ISO/IEC 27000 выделяется группа стандартов незаменимых при решении задачи оптимизации риска в облачных информационно-телекоммуникационных системах:

- ISO/IEC 27004:2009. — Information security management — Measurement. Руководство для выбора, проектирования, управления, улучшения средств и методов измерения эффективности и результативности СЗИ;

- ISO/IEC 27005:2011. — Information security risk management. Этот стандарт один из самых значимых в серии ISO/IEC 27000 и регламентирует процедуры управления

рисками.

- ISO/IEC 27002:2005. — Code of practice for information security management. Стандарт, который определяет ключевые положения при разработке, внедрении и для поддержки системы управления информационной безопасности (СУИБ),

Стандарт ISO/IEC 27005 раскрывает суть управления рисками информационных систем. Дает подробное описание критериям и подходам к оценке рисков. Вопрос оптимизации или минимизации риска также рассмотрен стандартом ISO/IEC 27005.

Оценивают риски нарушения информационной безопасности (ИБ) согласно следующим этапам:

- идентифицировать активы поставщика услуг и нарушителей информационной безопасности;

- идентифицировать существующие нормативные требования информационной безопасности;

- идентифицировать угрозы информационной безопасности;

- оценить возможности осуществления угроз ИБ с использованием шкалы значений «низкая», «средняя», «высокая»;

- оценить уязвимости информационной безопасности информационно—телекоммуникационных систем;

- оценить стоимость активов, используя данную шкалу;

- вычислить риски информационной безопасности по значениям от «0» до «8» либо применяя другие количественные значения.

ГОСТ Р 51624:2000. «Защита информации. Автоматизированные системы в защищенном исполнении». Стандартом устанавливаются общие требования по сохранности информации к автоматизированным системам в защищенном исполнении, применяемых в различных сферах деятельности. Стандарт принят к исполнению на всей территории Российской Федерации организациями и предприятиями, которые в своей деятельности применяют внедрение и эксплуатацию автоматизированных систем в защищенном исполнении. В ГОСТ Р 51624:2000 описаны важнейшие функции, которые подлежат к исполнению в автоматических системах защиты информации.

В стандарте ISO/IEC 31010:2009. «Менеджмент риска. Методы оценки риска» содержится принципы, руководствуясь которыми можно определиться с выбором и применением систематических методик оценки риска.

В работе, помимо технических стандартов, автор использовал информацию следующих международных нормативных документов:

- NIST SP 800-55. Показатели эффективности для информационной безопасности.

- NIST SP 800-53A. Оценка средств управления безопасностью в Федеральных информационных системах США;

- NIST SP 800-39. Управление рисками информационной безопасности;

- NIST SP 800-30. Руководство по управлению рисками.

В дальнейшем необходимо совершенствовать нормативно —методическую базу для использования облачных технологий. А на текущем моменте есть возможность использовать информацию следующих основополагающих документов:

- NIST SP 800-144 «Guidelines оп Security and Privacy in Public Cloud Computing». В сфере развертывания, эксплуатации и обеспечения информационной безопасности облачных сервисов хранения на текущий момент выступает основным нормативно— методическим документом.

- NIST SP 800-145 «The NIST DeГinition of Cloud Computing». В сфере облачных вычислений раскрывает смысл важнейших определений и терминов.

- NIST SP 800-146 «Cloud Computing Synopsys and Recommendation». Документ располагает общими сведениями об облачных технологиях, рекомендует методы эксплуатации. Также поднимается вопросы об оценке данных рисков в условиях использования облачных сервисов хранения;

- CSA «Security Guidance for critical areas of focus in cloud computing». Этот документ разработала частная организация Cloud Security Alliance. Альянс поставщиков и пользователей облачных информационно— телекоммуникационных систем для построения системы защиты информации облачного сервиса хранения разработал комплект рекомендаций.

- SLA. «Соглашение об уровне услуг». Для урегулирования обязанностей сторон в сфере облачных ИТКС документ SLA. «Соглашение об уровне услуг», является

основным документом. Формальный договор между заказчиком и поставщиком, согласно с методическими рекомендациями ITIL, SLA, является договор, который содержит описание предоставляемой модели обслуживания, прав и обязанностей обеих сторон, согласованный, качественный уровень предоставления услуг сервиса в сфере облачных ИТКС. Документ SLA. «Соглашение об уровне услуг», представляет собой основной инструмент, позволяющий постоянно анализировать и управлять качеством предоставляемых услуг аутсорсингом.

При рассмотрении действующих нормативно-правовых документов обнаружено, что они в вопросах обеспечения информационной безопасности в сервисах облачного хранения имеют определенные недоработки на текущий момент:

- отсутствие наличия системного подхода, собственно методологии построения системы защиты информации облачных информационно-телекоммуникационных систем;

- недостаточно проработаны вопросы моделей системы защиты информации и системы количественных метрик СЗИ облачного сервиса хранения;

- применение статистических подходов к оценке защищенности информационно-телекоммуникационных систем;

- отсутствие механизма подтверждения качества и надежности системы защиты информации.

Глава 2. Безопасность хранения данных в «облаках»

2.1. Преимущества и недостатки облачных хранилищ данных

Помимо некоторых очевидных плюсов облачные хранилища данных имеют недостатки и проблемы.

Преимущества:

- Доступ к данным везде, где есть доступ в Интернет.

- Большинство сервисов предоставляют более чем достаточный объем памяти.

- Высокая защита данных.

- Экономия места на жестком диске, что увеличивает скорость считывания информации с жесткого диска.

Недостатки:

- Возникает возможность хищения информации при передаче данных.

- В зависимости от услуг провайдера также может произойти утечка данных.

При выборе того или иного сервиса «облаков», чаще всего обращают внимание только на объём памяти, который можно получить бесплатно. Но при этом необходимо обращать внимание и на безопасность хранения данных.

При выборе облачного хранилища, сначала нужно узнать, шифруются в этом сервисе данные или нет.

Также стоит учесть, что если есть хоть малейшая вероятность появления личной информации в свободном доступе в сети Интернет, не стоит стопроцентно полагаться на защиту своих сведений в службах Интернет, в том числе и облачных хранилищах данных (даже включая те, которые используют шифрование).

2.2. Безопасность данных в OneDrive

Безопасность файлов в OneDrive обеспечивается несколькими способами:

- другие пользователи не имеют доступа к данным, если они не сохранены в общей папке или же не предоставлен общий доступ к выбранным файлам;

- сервис сохраняет несколько копий каждого файла на разных жестких дисках и серверах, что позволяет защитить данные пользователя, которые хранятся в OneDrive, в случае сбоя оборудования.

Чтобы защитить свои файлы в OneDrive, можно сделать следующее:

- придумать надежный пароль. Проверить надежность пароля;

- добавить сведения для защиты учетной записи Майкрософт: номер телефона, запасной адрес электронной почты, контрольный вопрос и ответ на него. Так, если пользователь вдруг забудет свой пароль или учетную запись взломают, служба сервиса сможет использовать эти сведения для подтверждения личности пользователя и поможет вернуть учетную запись и все то, что с ней связано;

- использовать двухшаговую проверку для входа в учетную запись. Безопасность учетной записи повысится благодаря дополнительному коду, который потребуется вводить каждый раз, когда пользователь будет входить не с доверенного устройства;

- архивировать файлы OneDrive.

2.3. Безопасность данных в Dropbox

Облачное хранилище данных Dropbox заботится о безопасности и конфиденциальности всей информации пользователя. В целях безопасности хранения данных этим сервисом приняты следующие меры:

- все данные проходят по защищенному SSL соединению;

- как утверждает компания, информация сохраняется на сервере в зашифрованном виде (AES-256), и персонал Dropbox не имеет доступа к этим файлам;

- доступ к общедоступным папкам могут получить только те пользователи, которые получили приглашение;

- доступ к файлам в контрольной папке получают только те пользователи, которые имеют ссылку на файл. Просмотреть всю папку или другие файлы в этом каталоге невозможно.

То есть, пользуясь облачным сервисом, пользователь получает комфорт, быстроту и полную безопасность во время доступа к информации любого компьютера или мобильного устройства, какие подключены к его аккаунту. Среди преимуществ Dropbox следует выделить то, что пользоваться сервисом может даже неподготовленный человек, и процедура использования данного приложения максимально упрощена. Сложные и длительные настройки полностью исключены.

Глава 3 Сравнительный анализ сервисов Dropbox и Microsoft SkyDrive

В данном разделе приведено небольшое сравнение облачных хранилищ данных Dropbox и Microsoft OneDrive.

Наиболее важными критериями оценки «облака» являются: время загрузки файла (коэффициент х время), бесплатное доступное пространство, максимальный размер одной загрузки, поддерживаемая операционная система, браузер, возможность редактирования документов в онлайн-режиме и экстренное восстановление предыдущих версий файлов.

Таблица 1

Сравнительные характеристики Dropbox и OneDrive

Особенности	Dropbox	OneDrive
Время загрузки файла (коэффициент х время)	1,32	2,14
Бесплатное доступное пространство (ГБ)	16	15
Максимальный размер одной загрузки (ГБ)	∞	10
Поддерживаемая операционная система	Windows, Mac OS, Linux, Android, iPhone, iPad, BlackBerry, Kindle Fire	Windows, Mac OS, iOS, Android, Xbox (One, 360)
Браузер	+	+
Встроенные редакторы	-	+

Экстренное восстановление предыдущих версий файлов	30 дней	30 дней

Исходя из представленных данных, можно сделать вывод, что различные хранилища данных имеют как неоспоримые преимущества перед другими сервисами, так и недостатки.

Заключение

В заключении нужно сказать, что «облачные хранилища данных» просто необходимы в наше время. В подтверждение этому можно привести ряд причин: нехватка мест на жестком диске, недолговечность ОС, «беготня с флэш картой» и так далее.

Облачные хранилища данных – это онлайн-сервис, который дает возможность хранить файлы на удаленном сервере в сети Интернет. Главный плюс этого сервера в том, что доступ к данным возможен из любой точки земного шара, где есть Интернет. Главный минус – это безопасность и конфиденциальность при передаче или получении данных.

Самыми известными хранилищами данных в «облаках» являются: Dropbox (хотя, в Dropbox нет возможности редактирования документов, зато здесь нет и никаких ограничений на формат и размер мультимедийных файлов), Microsoft OneDrive (в первую очередь беззаботное будущее сервиса связано с тесной интеграцией в Windows 8).

И в заключение, Dropbox – это многофункциональный и простой инструмент для обмена информацией, который одним из первых появился в сети Интернет. Увеличение количества пользователей дает возможность получить дополнительный объем памяти за счёт приглашенных друзей. Безопасность Dropbox находится на должном уровне: четырехзначный защитный код для мобильного приложения. Одно из преимуществ Dropbox заключается в том, что он, в отличие от Microsoft OneDrive, по умолчанию поддерживает Linux и Blackberry.

OneDrive – веб-приложение Microsoft, которое дает возможность онлайн-редактирования приложений Microsoft Office и имеет похожие настройки в предоставлении доступа к файлам с возможностью одновременного

редактирования.

В числе свойств, характерных только для OneDrive – это осуществление удаленного контроля над файлами с персонального компьютера, встроенная поддержка Window Phones и возможность делать синхронизированные заметки на мобильном устройстве через приложение OneNote.

К сожалению, нельзя считать облачные хранилища данных стопроцентно безопасными.

Именно поэтому следует во внимание взять некоторые советы.

1. Никогда не следует хранить в «облаках» важную информацию. Лучшее место для хранения данных – это рукописный блокнот, либо USB-флешка, к которой ни у кого нет доступа.

2. Если всё-таки нужно загрузить в «облако» важный файл, то прежде, чем сделать это, нужно зашифровать его. Самый простой способ – создать архив со сложным паролем.

3. Наилучший вариант использования «облаков» – это хранение музыки, фильмов, электронных книг. Именно в этом отношении облачные сервисы и следует использовать.

Список литературы

1. Андреев В. Защита виртуальной инфраструктуры / В. Андреев, І. Корчагин, А. Ковязин; IT-Expert. – Вип. 6, 2011. – С. 64-69.

2. Батаев, А. В. Перспективы внедрения облачных технологий в банковском секторе России, «Научно-технические ведомости Санкт-Петербургского государственного университета», №2 (192), 2014, с. 156–165

3. Батаев, А. В. Тенденции и перспективы развития рынка информационных технологий в банковском секторе России, Молодой ученый. — 2013. — №10, с. 268–271

4. Безопасность цикла разработки приложений корпорации Microsoft SDL — обеспечение безопасности в процессе разработки Windows Azure: www.microsoft.com/security/sdl/

5. Белов Е.Б., Лось В.П. Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М.:Горячая линия — Телеком, 2006.

6. Войтик А.И., Прожерин В.Г. Экономика информационной безопасности.

7. Всемирный фонд службы безопасности корпорации Microsoft — разработка доверенной и доступной в сети среды, лежащей в основе Windows Azurehttp: http://www.globalfoundationservices.com/security/

8. Герасименко В.А., Малюк А.А. Основы защиты информации. —М.: МИФИ, 1997.

9. ГОСТ Р 50922—2006. Защита информации. Основные термины и определения. — Введен 2006.

10. ГОСТ Р 51583. Порядок создания автоматизированных систем в защищенном исполнении. — Введен 2000.

11. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — Введен 2008.

12. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. — Введен 30.10.2010. —М.: Стандартинформ, 2011.

13. Демурчев Н. Г. Проблемы обеспечения информационной безопасности при переходе на облачные вычисления / Н. Г. Демурчев, С. О. Ищенко; Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. Таганрог: Изд-во ТТИ ЮФУ, 2010.

14. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ТИД «ДС», 2008.

15. Домашняя страница Windows Azure — общая информация и ссылки на ресурсы, посвященные Windows Azure: http://www.microsoft.com/windowsazure/

16. Кондратьев, А. А., Тищенко И. П., Фраленко В. П. Разработка распределенной системы защиты облачных вычислений, «Программные системы: Теория и приложения», №4 (8), 2011, с. 61–70

17. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы информационной безопасности. —М.: Горячая линия —

Телеком, 2004.

18. Остапенко Г.А. , Карпеев Д.О., Плотников Д.Г и др. Риски распределенных систем: методики, алгоритмы оценки и управления// Информация и безопасность. 2010. If 4. С.485—530

19. Приказ ФСБ РФ N 796. «Об утверждении требований к средствам электронной подписи и требований к средства удостоверяющего центра» — Введен 27 декабря 2011.

20. Рекомендации по безопасности при разработке приложений Windows Azure: http://download.microsoft.com/download/7/3/E/73E4EE93-559F-4D0F-A6FC-7FEC5F1542D1/SecurityBestPracticesWindowsAzureApps.docx

21. РС БР ИБСС-2.2—2009. Методика оценки рисков нарушения информационной безопасности. — Введен 2010.

22. Руководящий документ Гостехкомиссии России. «Автоматизированные системы защиты от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к защите»

23. Сертификация ISO 27001 Всемирного фонда службы безопасности корпорации Microsoft: http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search- Results/?pg = 1&licencenumber=IS+533913&searchkey=companyXeqXMicrosoft

24. Службы криптографии и защита данных в Windows Azure: http://msdn.microsoft.com/en-us/magazine/ee291586.aspx

25. Статья. Автоматизированная банковская система: стоимость. [Электронный ресурс]. Режим доступа: http:// www.absonline.ru/software/cost/(Дата обращения 22.04. 2017)

26. Статья. Аутсорсинг АБС — осознанная необходимость. Банковское обозрение. [Электронный ресурс]. Режим доступа: http://bosfera.ru/bo/2013/07/autsorsing-abs (Дата обращения 22.04. 2017)

27. Статья. Облачные вычисления (мировой рынок). [Электронный ресурс]. Режим доступа: http://www.tadviser. ru/index. php/Статья: Облачные_вычисления_ (мировой_рынок) (Дата обращения 22.04. 2017)

28. Статья. Облачные сервисы (рынок России). [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index. php/(Дата обращения 22.04. 2017)

29. Структура облачных сервисов ЦФТ. М.: ЦФТ, 2013. — 36 с.