МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Защита информации при использовании облачных сервисов»

Исполнитель Крутилина Анастасия Сергеевна
(фамилия,имя,отчество)

Руководитель
(ученая степень, ученое звание)

Алейникова Оксана Вячеславовна
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____
(подпись)

профессор, доктор технических наук
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«17» февраля 2017 г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Защита информации при использовании облачных сервисов»

Исполнитель Крутилина Анастасия Сергеевна
(фамилия,имя,отчество)

Руководитель
(ученая степень, ученое звание)

Алейникова Оксана Вячеславовна
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

профессор, доктор технических наук
(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«__»_____20__г.

Санкт–Петербург

2017

Оглавление:

Введение

В настоящее время информация является одним из наиболее важных ресурсов не только для конкурирующих за влияние на рынке компаний, но и для целых государств. При этом обработка и хранение данной информации нуждается в значительном количестве мощности вычислительных машин. Поэтому требования к ним увеличиваются с поразительной скоростью. А вместе с тем и стоимость.

Большие объемы вычислительной мощности требуются не только для торговых промышленных предприятий, но и в областях образования и развлечений. Поэтому все острее встает вопрос о необходимости создания экономичных и эффективных систем обработки данных.

В связи со стремительным развитием технологий беспроводного доступа отпала необходимость расположения комплекса средств обработки и хранения информации непосредственно на территории организации и стала возможной удаленная работа с данными. Это дало первый толчок к возникновению облачных сервисов.

На сегодняшний день облачные вычисления являются одним из наиболее перспективных направлений развития информационных технологий, и рассматриваются в качестве альтернативы традиционным способам работы с информацией. Использование структуры облачных вычислений позволяет реализовать возможность удаленной работы с информацией и обеспечивает достижение высоких показателей доступности и отказоустойчивости.

В прошлом году общий объем мирового рынка в сфере облачных технологий занял порядка $40 млрд. Большинство экспертов прогнозируют, что к 2020 году это значение достигнет $240 млрд.

На данный момент, в Российской Федерации активно развивается большое количество компаний, предоставляющих облачные услуги. В

настоящее время Россия по внедрению облачных сервисов в бизнес занимает 34-е место с показателем $250 млн.

В связи с активным развитием данной отрасли, сохранение безопасности при хранении и передачи данных является одной из главных проблем при работе с облачными системами, особенно в отношении сведений, содержащих коммерческую тайну или иную защищаемую информацию.

Поэтому целью данной выпускной квалификационной работы является выбор оптимальных методов защиты данных пользователя, использующихся в облачных сервисах.

Для достижения поставленной цели необходимо решить следующие задачи:

— Рассмотреть особенности построения облачных сервисов;

— Исследовать проблематику защиты информации в облачных технологиях;

— Рассмотреть существующие методы защиты информации при работе с облачными технологиями.

При написании данной работы могут возникнуть трудности, связанные с отсутствием в свободном доступе полной информации о конфигурации и стоимости предоставляемых услуг поставщиками.

1 Описание облачных сервисов

1.1 Характеристики облачных сервисов

Облачные вычисления (от англ. cloud computing, также используется термин «облачная обработка данных») - это инновационный подход к модели представления IT инфраструктуры, предоставляющей пользователям комплекс взаимосвязанных информационных систем для коллективного дистанционного доступа к данным. Данный комплекс состоит из совокупности аппаратных и сетевых ресурсов, а также программного обеспечения, базирующегося на удаленных DATA центрах поставщиков. Таким образом, потребителю могут быть быстро предоставлены масштабируемые вычислительные ресурсы и программное обеспечение в виде услуги, а обязанности по выбору компьютеров, обрабатывающих запросы, и управляющей операционной системы возлагаются на поставщика облачных услуг. Основной составляющей облака является технология виртуализации, которая позволяет пользователям использовать вычислительные ресурсы на любой платформе независимо от аппаратной реализации и помогает распределять вычислительную мощность, необходимую клиентам, на несколько серверов, возможно даже территориально отдаленных друг от друга[1]. При этом все вычислительные процессы будут логически изолированы друг от друга.

Появление концепции облачных вычислений является результатом развития информационных технологий за последние несколько десятилетий и стремительным ростом глобализации. Термин же появился благодаря буквальному словесному описанию картинок из книг, в которых рабочая станция пользователя соединялась с сетью, схематично изображаемой в виде облака.

Впервые идея о том, что «компьютерная технология разделения времени может привести к будущему, в котором компьютерная мощь и даже определенные приложения могут продаваться с использованием бизнес-модели

сферы услуг», была высказана в 1961 году американским информатиком Джоном Маккарти[2]. Появление универсальной компьютерной системы IBM System/360 в 1964 году дало начало мэйнфреймам, с которыми часто сравнивают облачные сервисы. Но между ними существует два принципиальных отличия. Во-первых, теоретически вычислительная мощность облачной системы не имеет ограничений при соблюдении необходимых условий эксплуатации. Во-вторых, терминалы для работы с мэйнфреймами предназначены непосредственно для диалоговой связи пользователя с обрабатываемой задачей. А в облачных системах терминал изначально представляет собой полноценное средство работы, способное не только сохранять информацию в буфере, но и напрямую осуществлять управление глобальным комплексом вычислительных ресурсов.

С 1990-го года стали широко использоваться grid-вычисления. Этот способ обработки данных предполагает под собой систему аренды вычислительной мощности свободных ресурсов процессоров. На данный момент эта форма распределенных вычислений все еще применяется для решения научных задач, где требуются значительные вычислительные ресурсы. И несмотря на то, что облачные системы и Grid-вычисления схожи в принципах построения и эксплуатации, первые считаются наиболее перспективными благодаря более развитым функциям удаленной работы.

Новый этап развития технологий обработки данных начался с наступлением 21 века, когда программные и аппаратные средства совершили значительный прорыв вперед. Так в 2006 году компания Amazon представила свою инфраструктуру веб-сервисов под названием Elastic Computecloud (EC2), предоставляющую не только услуги по размещению информации и приложений пользователей на сервере, но и возможность их удаленной обработки[2]. С тех пор идеология облачных вычислений ежегодно набирает популярность благодаря быстрому развитию каналов связи и стремительно растущим потребностям пользователей. На сегодняшний день облачные

сервисы представляют собой тысячи серверов, размещенных в центрах обработки данных (ЦОД), и обеспечивающих ресурсами десятки тысяч приложений, которые одновременно используют миллионы пользователей.

Для того чтобы система вычислений могла считаться облачной, она должна соответствовать пяти обязательным характеристикам, которые были установлены Национальным институтом стандартов и технологий США[3].

1) Самообслуживание по требованию — потребитель по мере необходимости может лично выбирать и изменять такие параметры системы, как серверное время, скорость доступа и обработки данных, объём хранимых данных без взаимодействия с представителем поставщика услуг;
2) Универсальный доступ по сети — запрашиваемые услуги доступны потребителям по сети передачи данных в любой точке мира вне зависимости от используемого терминального устройства;
3) Объединение ресурсов — поставщик услуг объединяет ресурсы для обслуживания большого числа потребителей в единый пул для динамического перераспределения мощностей между потребителями в условиях постоянного изменения спроса на мощности; при этом потребители контролируют только основные параметры услуги;
4) Эластичность — область предоставляемых услуг может быть расширена или сужена в любой момент времени в автоматическом режиме;
5) Учёт потребления — поставщик автоматически оценивает объем предоставленных потребителям услуг (например, объём хранимых данных, пропускная способность, количество пользователей, количество транзакций), и на основе этих данных рассчитывает стоимость использования.

Для потребителя соблюдение данных характеристик дает гарантию того, что им будут предоставлены автоматически масштабируемые услуги с высоким уровнем доступности и низкими рисками неработоспособности без

необходимости создания, обслуживания и модернизации собственной аппаратной инфраструктуры. Удобство и универсальность доступа обеспечивается широкой доступностью услуг и поддержкой различного класса терминальных устройств (персональных компьютеров, мобильных телефонов, планшетов).

В то же время для поставщиков облачных вычислений появляется возможность проектирования новой бизнес-модели предоставления серверного оборудования, позволяющей экономить на масштабах, используя меньшие аппаратные ресурсы, чем требовались бы при выделенных аппаратных мощностях для каждого потребителя, благодаря объединению ресурсов и непостоянному характеру потребления со стороны потребителей. А за счет автоматизации процедур выделения ресурсов существенно снижаются затраты на абонентское обслуживание[4].

Использование облачных сервисов или отказ от них зависит исключительно от нужд пользователей. В том случае, если компания или частный клиент уверены в необходимости использования данной модели предоставления услуг, первым шагом создания облачной системы для них будет являться выбор модели развертывания.

1.2 Модели развертывания облачных систем

На данный момент выделяют три модели развертывания облачных систем. Они подразделяются на частные, публичные и гибридные.

Частное облако – это внутрикорпоративная облачная инфраструктура, предназначенная для обслуживания конкретного предприятия и его филиалов. Частное облако может непосредственно управляться заказчиком или быть поручено внешнему подрядчику. От этого зависит размещение аппаратной инфраструктуры, которая может быть расположена как на территории клиента, так и внешнего оператора. Также возможен вариант разделения, когда часть аппаратных средств находится у заказчика, а часть у оператора. Идеальный

вариант частного облака – облако, развернутое на территории организации, обслуживаемое и контролируемое ее сотрудниками.

Преимуществом модели частного облака перед остальными является возможность осуществления более детального контроля над предоставляемыми ресурсами и расширенные возможности их конфигурации. Кроме того, частные облака являются идеальным решением в случае выполнения работы с конфиденциальной информацией[5]. Но, в то же время это может считаться основным недостатком, так как предприятие должно иметь возможность самостоятельно установить и поддерживать облачные сервисы. В этом случае расходы, связанные с созданием и эксплуатацией, ложатся на компанию и могут превышать ценность обрабатываемой информации.

Частным случаем такой инфраструктуры можно считать облако сообщества (Community cloud), предназначенное для совместного использования вычислительной мощности частного облака несколькими организациями или лицами, разделяющими одни интересы и требования к политике безопасности и руководящим документам[6].

Публичное облако – это облачная инфраструктура, находящаяся в полном распоряжении поставщика услуг и предназначенная для свободного использования широкой публикой. Вся ответственность по установке, обслуживанию и поддержанию работоспособности возлагается на провайдера. Клиенты, использующие возможности данного типа инфраструктуры, не имеют доступа к управлению и конфигурированию системы и фактически оплачивают только используемые ресурсы в виде вычислительной мощности и абонентского доступа. Абонентом данного типа сервисов может стать как компания, так и индивидуальный пользователь.

Основными преимуществами публичных облаков являются большая возможность масштабирования в сравнении с другими сервисами и доступность по стоимости для рядового пользователя, за счет оплаты только потребляемых ресурсов[7].

При этом главным недостатком данной инфраструктуры является наименьшая возможность конфигурирования системы со стороны клиентов, так как данные функции обычно являются стандартизированными и основываются на наиболее часто запрашиваемых пользователями случаях. Также не стоит упускать из виду, тот факт что, поскольку потребители не имеют возможности управления инфраструктурой, информация, нуждающаяся в повышенных требованиях безопасности и нормативного контроля, не может находиться в общедоступном облаке из-за ограниченной ответственности поставщика в этом вопросе.

Гибридное облако - это инфраструктура, представляющая из себя сочетание общедоступных и частных моделей облаков. В данном типе систем обязанности по управлению распределяются между провайдером и клиентом. Данный сервис предоставляет услуги, относящиеся как к частным, так и публичным облакам[8]. Наибольшую популярность этот тип сервиса имеет у организаций, имеющих повышенный уровень активности в определенные периоды времени. Благодаря нему компании могут отправлять часть не имеющей ценности информации на публичное облако во время ресурсозатратной обработки важных сведений, а также предоставлять через него доступ пользователям к ресурсам предприятия, находящимся в частном облаке. Превосходно рассчитанное облако данного типа позволяет обрабатывать как информацию, имеющую повышенные требования к безопасности, так и более незначительную.

Так как подобная концепция является новым решением в сфере облачных вычислений, фундаментальным недостатком гибридных облаков является трудность создания оптимального решения по реализации данной инфраструктуры. Претворение в жизнь осложняется как конфигурацией взаимодействия между частным и общедоступным компонентами, так и настройкой получения услуг из разных источников и объединением их в единый блок[9].

После рассмотрения достоинств и недостатков трех существующих моделей развертывания облачной инфраструктуры можно выделить модель частного облака, как наиболее безопасную и обеспечивающую больше возможностей для конфигурации системы.

Следующим шагом реализации облачного сервиса является выбор модели обслуживания, предоставляемой провайдером облачных услуг.

1.3 Модели обслуживания

В настоящее время существует несколько моделей обслуживания со стороны поставщика[9]. Их принято разделять на три группы в зависимости от типа предоставляемых услуг (Рисунок 1). Подобные модели иногда даже называют слоями облака, хотя считается, что они отражают строение информационных технологий в целом.

Рисунок 1 – Модели обслуживания

Инфраструктура как услуга (Infrastructure as a Service – IaaS) - это модель предоставления клиентам набора физических ресурсов центра обработки данных, таких как серверы, сетевое оборудование и устройства хранения. При этом потребитель не может контролировать облачную инфраструктуру, однако может управлять операционными системами, системами хранения, развернутыми приложениями и некоторыми сетевыми компонентами. В этом случае защиту платформ и приложений клиент обеспечивает самостоятельно, а на провайдера возлагается организация защиты инфраструктуры.

Частным случаем инфраструктуры как услуги является аппаратное обеспечение как услуга (Hardware as a Service – HaaS), где пользователь получает оборудование, на основе которого разворачивает свою собственную инфраструктуру с использованием наиболее подходящего программного обеспечения.

Эта модель часто подразумевает использование методов виртуализации, поэтому ее основным преимуществом можно считать снижение инвестиций в оборудование. А к недостаткам относиться то, что бизнес-эффективность и производительность в значительной степени зависит от возможностей поставщика. Также есть вероятность, что потребуются потенциально крупные долгосрочные затраты и дополнительные меры по обеспечению безопасности.

Платформа как услуга (Platform as a Service – PaaS) – это модель предоставления пользователю инфраструктуры для размещения созданных или приобретенных приложений, таких как программное обеспечение, мессенджер, хранилище данных, без возможности управления инфраструктурой в целом. В данном случае клиент не имеет возможности конфигурировать базовую структуру облачного сервиса, но ему дается доступ к настройке параметров хостинга и установленных приложений. Обеспечение безопасности хранимой и обрабатываемой информации также возлагается на пользователя.

Предоставляемые приложения могут функционировать как в центрах обработки данных компании, так и непосредственно в облаке благодаря

технологии виртуализации. Частными случаями PaaS являются такие услуги как:

1) Рабочее место как услуга (Workplace as a Service – WaaS) - модель предоставления компаниям стандартизированного программного обеспечения, доступного для всех сотрудников независимо от используемой ими аппаратной части.
2) Данные как услуга (Data as a Service – DaaS) - модель предоставления пользователю дискового пространства, которое может быть использовано для хранения личной информации или сохранения резервных копий системы и приложений.
3) Безопасность как услуга (Security as a Service – SaaS) - модель предоставления пользователю возможности развертывания системы безопасносности предприятия, связанной с использованием веб-сервисов.

Основными преимуществами данной модели является отсутствие необходимости переплачивать провайдерам за неиспользуемые ресурсы, а также плавность развертывания приложений и набор средств для создания, тестирования и выполнения программного обеспечения. Недостатки заключаются в отсутствии контроля и управления физической и виртуальной инфраструктурой облака и обеспечения безопасности со стороны поставщиков.

Приложение как услуга (Software as a Service – SaaS) - это модель предоставления пользователю программного обеспечения, развернутого на удаленных серверах поставщика, как сервиса, доступ к которому осуществляется посредством Интернета, При этом все проблемы, связанные с обновлением и лицензированием приложений возлагаются на провайдера данной услуги. Программное обеспечение в данном случае оплачивается по факту использования или предоставляется на безвозмездной основе, но с условием возможности получения дохода от рекламы.

Предоставляемые приложения могут быть доступны посредством различных клиентских устройств, всемирной паутины или мобильных приложений. Ответственность клиента заключается только в сохранении параметров доступа и выполнении рекомендаций провайдера по безопасным настройкам приложений.

Преимуществом данной услуги является удобный доступ к работе через интернет или мобильное приложение, а недостатками невозможность управления инфраструктурой облака. низкая скорость обработки данных в реальном времени и запрет на обработку данных на сторонних сервисах.

Тенденции развития технологий говорят о том, возможно в скором времени подобное разделение не будет иметь смысла, так как появятся поставщики, предоставляющие и программную и аппаратную часть, а также функции управления инфраструктурными и платформенными элементами, собранные от разных поставщиков, но объединенные в единую облачную систему. Данная концепция имеет название «Всё как услуга» (Everything as a Service).

2 Основные угрозы и методы их устранения

2.1 Угрозы

В настоящее время облачные вычисления являются прогрессивным методом оптимизации IT инфраструктуры. Но, несмотря на все положительные моменты это влечет за собой ряд проблем, связанных как с трудностью сохранения конфиденциальности обрабатываемых данных, так и с областью ответственности провайдеров. В интересах поддержания собственной репутации провайдеры много внимания уделяют обеспечению безопасности данных от возможного проникновения извне. Но не всегда такое же внимание уделяется юридическим аспектам использования данных самим поставщиком. А в отдельных случаях (например в общедоступных сервисах облачного хранения, таких как Google и т.д) даже напрямую указывается тот факт, что поставщик имеет право использовать любую полученную от пользователя информацию так, как сочтет это нужным. Поэтому так важно знать способы обеспечения безопасности обрабатываемых данных.

За основу обеспечения физической безопасности берется строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличие от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и брандмауэр.

В настоящее время не один облачный провайдер не может гарантировать, что учтены все ресурсы предоставляемого им облачного сервиса и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака. Поэтому важно знать, с какими опасностями может столкнуться пользователь при использовании облачных систем.

2.1.1 Угрозы виртуализации

Как уже упоминалось ранее, облачные среды можно разделить на три категории в соответствии с тремя моделями развертывания. Но в каждой из них важнейшая роль отводится технологии виртуализации. Требования к безопасности облачных систем мало отличаются от требований, предъявляемых к работе обычных центров обработки данных. Однако переход к виртуализации может стать причиной возникновений новых типов угроз. Поэтому рассмотрим основные возможные угрозы, возникающие в системе облачных вычислений[10].

В настоящее время эта вычислительная платформа имеет следующие потенциально слабые стороны:

— Обмен данными между разными виртуальными машинами или между виртуальной машиной и хостом с применением совместно используемых дисков, виртуальных коммутаторов или виртуальных локальных сетей (VLAN) и совместно используемой подсистемы ввода-вывода или кэша.

— Стандартные драйверы, эмулирующие аппаратные средства.

— Уязвимости в гипервизоре, которые позволяют выполнять произвольный код на хосте с привилегиями гипервизора, что дает злоумышленнику возможность осуществлять управление всеми виртуальными машинами и самим хостом.

— Руткиты, позволяющие получить управление системой и вносить изменения в работу гипервизора в целях внедрения и выполнения вредоносного кода.

— «Побег из виртуальной машины» - уязвимость, предоставляющая программе выход из виртуальной машины и возможность взаимодействия с операционной системой, а также безграничный доступ к хосту благодаря совместно используемым ресурсам.

— Атаки типа «отказ в обслуживании», заключающиеся в выведении из строя одной виртуальной машины, через которую в дальнейшем совершается нападение на остальные машины, запущенные с ней на одном хосте.

Первым шагом к принятию мер защиты в отношении этих угроз является понимание рабочей среды. Если данные должны быть защищены в соответствии с законами, стандартами или отраслевыми нормами, то к обеспечению безопасности должен быть применен соответствующий подход, уделяющий внимание конкретно этому типу используемой среды. И в этом случае наиболее предпочтительным является решение, основанное на модели частного или гибридного облачного сервиса, в котором все нуждающиеся в безопасности данные располагаются на территории подконтрольного ведомства, и находятся непосредственно под охраной организации-правообладателя.

Следующим шагом является проверка поставщика облачных услуг на предмет надежности и выяснение предпринимаемых мер для защиты наиболее уязвимых мест в системе, особенно в отношении гипервизора.

Гипервизор является одним из ключевых элементов виртуальной системы. Его основная функция заключается в распределении ресурсов между виртуальными машинами, обеспечивая тем самым работу нескольких операционных систем и изолируя, их друг от друга. И вывод гипервизора из строя может привести к тому, что одному пользователю станут доступны не только физические ресурсы и память другого, но и возможность перехвата сетевого трафика. Поэтому информация о типе используемого поставщиком программного обеспечения, осуществляющего виртуализацию, а также расписание внесения исправлений и обновлений подлежат обязательному выяснению. Кроме того, необходимо убедиться в том, что гипервизор сконфигурирован для обнаружения экстремального потребления ресурсов в целях защиты от атак типа «отказ в обслуживании».

В качестве стандартных методов защиты рекомендуется применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога Active Directory, использование политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам хост-сервера, применять встроенный брандмауэр хоста виртуализации. Также возможно отключение таких часто неиспользуемых служб как, например, веб-доступ к серверу виртуализации.

2.1.2 Потеря и утечка данных

С момента появления данных в облаке, средства компании по предотвращению утечки данных считаются недействительными, так как уже не могут помочь в защите конфиденциальности этих данных. При этом, в большинстве случаев, компания даже не имеет возможности прямого контроля над сохранением безопасности своих данных не только в общедоступном облаке, но и в таких моделях предоставления услуг как «программное обеспечение как сервис» (SaaS) и «платформа как сервис (PaaS)»[11].

Для предотвращения утечки информации в облачных сервисах существует множество решений и готовых продуктов, но они в основном направлены на обеспечение целостности и доступности данных и не подходят для реализации защиты. Кроме того, эти решения не подходят для сред, где пользователь не имеет доступа к управлению инфраструктурой.

Между тем основой предотвращения утечки информации является применение доверенных систем хранения и транспортирования данных. Прежде всего, от поставщика требуется использование высоконадежного шифрования как во время хранения, так и во время передачи материала. Также необходимо иметь заверенное соглашение, в котором будут четко определены роли провайдера и потребителя в обеспечении безопасности данных, и условия предоставления сервиса. Помимо этого контракт должен содержать требование к поставщику услуг облака об уничтожении данных, хранящихся на

постоянных носителях, перед их освобождением в пул. В тоже время согласно требованиям стандарта PCI DSS, необходимым является наличие должным образом сконфигурированного межсетевого экрана Web-приложений для защиты последних от разнообразных атак, а также проведение испытания проникновением, чтобы проверить защиту от нежелательного доступа всех используемых компанией приложений.

Наконец, на стороне организации требуется наличие соответствующих политик безопасности. Компании, опасающиеся утечки информации, должны иметь действующие политики классификации данных и установления стандартов относительно порядка обращения с данными различного уровня конфиденциальности, которые могут оказаться абсолютно не предназначенными для хранения в облаке.

2.1.3 Незащищенные интерфейсы API

Для того чтобы клиентам было удобно взаимодействовать с облачными сервисами, поставщики услуг часто предоставляют интерфейсы прикладного программирования (API), которые могут быть применимы для управления и мониторинга облака. Поэтому в большей степени безопасность использования облачных услуг зависит от того, насколько качественно защищены данные интерфейсы API.

Серьезными угрозами безопасности в данном случае являются функции осуществления анонимного доступа, открытые способы аутентификации и многократное использование паролей, а также устаревшие средства контроля доступа и авторизации[12].

Кроме того, интерфейсы API, разработанные сторонними организациями для предоставления клиентам дополнительных возможностей использования облачных сервисов, не всегда отвечают требованиям безопасности и подвергаются детальному анализу, или даже могут содержать скрытые

функции передачи данных стороннему лицу. А это повышает уровень риска нарушения конфиденциальности.

Во избежание подобных проблем следует использовать только приложения, предоставляемые или проверенные поставщиком облачных услуг, а также удостовериться в том, что провайдер делает все необходимое для защиты таких интерфейсов API. Кроме того организация должна провести тщательную проверку средств аутентификации и доступа, чтобы быть уверенной в наличии шифрования данных при передаче. А так же убедиться, что используются только заявленные в договоре интерфейсы программирования.

2.1.4 Похищение и несанкционированное использование учетных записей

До настоящего времени были рассмотрены только уязвимости, борьба с которыми возлагается на плечи поставщика облачных услуг. Но обеспечение безопасности учетных записей пользователей в равной доле зависит и от провайдера облачных систем и от потребителя. Потому что уязвимости программного обеспечения, делающие возможным перехват учетной информации пользователя, не являются самым распространенным способом кражи аутентификационных данных.

В большинстве случаев, чтобы завладеть учетной информацией пользователей, злоумышленники используют фишинговые атаки, вредоносное программное обеспечение и социальную инженерию. А так как люди часто используют одни и те же имя пользователя и пароль для получения различных услуг, то только облегчают хакерам поиск аутентификационной информации. С момента получения злоумышленником учетных данных пользователя, под угрозу ставиться не только целостность и конфиденциальность данных, хранящихся в облаке, но и репутация компании, так как правонарушители могут использовать полученную информацию для проведения атак на другие организации[13].

Поэтому от организации требуется не только понимание политик безопасности поставщика облака, но и осуществление упреждающего мониторинга пользования облачными сервисами для отслеживания несанкционированного доступа и несанкционированной активности.

Также применение политик со стороны компании, предусматривающих использование уникальных учетных данных для входа в систему и надежных паролей, помогает предотвратить уязвимости, связанные с многократным использованием пользовательской информации. Еще больше уменьшить вероятность атак подобного типа помогают методы двухфакторной аутентификации.

2.1.5 Угрозы со стороны инсайдеров

Как правило, компании тратят очень много средств на установку систем защиты с разграничением доступа пользователям и проверку благонадежности сотрудников. Но когда речь заходит о действиях персонала со стороны поставщика облачных услуг и о том, как регламентированы их действия, прозрачность процессов и процедур, является недостаточной.

Передача управления сервисами поставщику облачных сервисов означает отсутствие у клиента представления о том, кто имеет доступ (физический и виртуальный) к ресурсам организации. Информация о контроле сотрудников, анализе и соблюдении политик безопасности, так или иначе, не является доступной для пользователей. А в то же время возможность работы с засекреченной информацией является очень привлекательной для хакеров и корпоративных шпионов, так как получение контроля над облачным сервисом предлагает злоумышленнику такие конфиденциальные данные, как объем продаж и прибыль компании, которые могут быть проданы им с незначительной долей риска обнаружения или вообще без такового.

Основной мерой защиты от вредоносной инсайдерской деятельности со стороны поставщика услуг является осведомленность о том, какие меры

контроля сотрудников предпринимаются провайдером, а также какие действия будут предприняты в случае нарушения защиты и утечки информации. Если сроки или процесс оповещения являются неприемлемыми, следует поискать какого-либо другого поставщика услуг.

2.2 Методы защиты

После рассмотрения существующих угроз в сфере облачных вычислений можно выделить несколько наиболее распространенных решений возникающих проблем. Проанализировав опубликованную по данному вопросу информацию и опираясь на методы защиты, выбранные организацией Cloud Security Alliance (CSA), было выделено четыре метода обеспечения безопасности информации в среде облачных технологий: шифрование, защита данных при передаче, аутентификация, изоляция пользователей.

2.2.1 Защита данных при передаче

Основным отличием облачных сервисов от обычных центров обработки данных является удобство доступа пользователя к ресурсам приложения в любой момент, из любого места и с любого устройства, имеющего доступ к сети интернет. Но помимо отдельных пользователей к облачной системе могут подключать свою локальную инфраструктуру целые компании. При этом и те, и другие должны быть абсолютно уверены в безопасной доставке своих данных до облачного сервиса. Поэтому рассмотрим возможные способы и варианты безопасного доступа с двух сторон.

Подключение конечных пользователей к облачным сервисам

Для подключения отдельных пользователей в настоящее время имеется несколько вариантов подключения к облачным сервисам, отличающихся друг от друга не только настройкой и установкой, но и удобством использования. Это подключение посредством RDP-клиента, RemoteApp, Веб-доступа, Remote access VPN, VPN site-to-site, DirectAccess и VDI[14].

1) Подключение посредством удаленного рабочего стола (RDP-клиент)

Удаленный рабочий стол - это инструмент удаленного доступа к рабочему месту созданный на основе проприетарного протокола прикладного уровня RDP (Remote Desktop Protocol). На данный момент существует множество клиентов для наиболее популярных операционных систем, с помощью которых пользователь подключается к удаленному рабочему столу и может запускать развернутые на сервере терминалов приложения, а также может конфигурировать параметры доступа и системы. Кроме того RDP клиент поддерживает функцию обмена данными между локальным компьютером и удаленным рабочим столом.

2) Удаленные приложения служб терминалов (RemoteApp)

Это решение является разновидностью рассмотренного выше варианта. Принципиальное отличие заключается только в том, что при доступе к удаленному рабочему столу пользователь имеет доступ к целой операционной системе и установленным на ней программам, а RemoteApp предназначен для доступа к конкретному приложению, интегрированному с рабочей станцией пользователя, но фактически располагающемуся на удаленном сервере. Средствами RemoteApp происходит подключение к данному серверу, авторизация и запуск программы, создавая видимость локально установленного приложения.

3) Веб-доступ к службам терминалов

Этот способ помогает осуществить доступ как к удаленному рабочему столу, так и к отдельному приложению посредством браузера. Для этого пользователю необходимо авторизоваться на веб-странице поставщика услуги.

4) Подключение по VPN

VPN - это виртуальная частная сеть, позволяющая обеспечить несколько надежных интернет соединений, используя различные средства криптографии.

Существует два типа VPN-туннелей:

— Remote access VPN - это защищенный туннель, организованный между приложением на компьютере клиента и каким-либо устройством (например,

маршрутизатором), расположенном в облаке хостинг-провайдера. Для реализации данного типа доступа пользователю необходимо запустить ярлык VPN на своей рабочей станции и ввести свои верительные данные. При успешной авторизации пользователь попадает в сеть виртуального удаленного офиса в облаке и может использовать ресурсы так, как если бы он находился непосредственно в офисе компании.

— Site-to-site VPN — это защищенный туннель, организованный между двумя устройствами пользователей, расположенными в одной локальной сети. Поэтому не требуется устанавливать на компьютерах какое-либо специальное программное обеспечения. Данный тип туннель применяется, если количество пользователей в компании, которым необходим доступ к ресурсам файлового сервера, достаточно велико. В этом случае необходимо непосредственно в офисе компании дополнительно развернуть VPN-сервер и реализовать подключение Site-to-Site VPN на уровне VPN-сервера в облаке и VPN-сервера в офисе компании.

5) DirectAccess

Помимо стандартных реализаций VPN существует технология DirectAccess, основанная на базе Microsoft. Она позволяет реализовать возможность удаленного доступа к ресурсам разворачивая туннель до сервера DirectAccess и благодаря нему получая доступ ко всей сети. При этом пользователю не нужно предпринимать никаких дополнительных действий. Даже если связь с Интернетом будет потеряна на какое-то время, туннель самостоятельно восстановится.

6) VDI (виртуализация рабочих столов)

На сегодняшний день виртуальная инфраструктура рабочих столов (VDI, Virtual Desktop Infrastructure) реализована на многих облачных площадках корпоративных IaaS-провайдеров и позволяет централизовать рабочие станции пользователей на серверах виртуализации, создав при этом единую точку управления, развертывания и обслуживания. Для реализации данной

технологии со стороны клиента требуется наличие интернет-соединения и рабочей станции. На практике выделяется сервер в облаке IaaS-провайдера, на который устанавливается гипервизор, а на нем разворачиваются отдельные виртуальные машины. На конечном устройстве пользователя запускается программа-клиент и происходит подключение к инфраструктуре.

Подключение локальной инфраструктуры компании к IaaS-инфраструктуре в облаке

Зачастую многие мелкие и даже средние компании не имеют своей локальной ИТ-инфраструктуры, предпочитая при этом развертывание всех необходимых для бизнеса решений и сервисов в облаке IaaS-провайдера. Такой подход экономически оправдан, выгоден и удобен.

Существует несколько возможных вариантов подключения локальной инфраструктуры компании к IaaS-инфраструктуре в облаке:

— аренда выделенного канала и подключение к ЦОД для доступа к облаку;

— проброс своего кабеля до ЦОД;

— использование точек обмена трафиком.

Рассмотрим каждый из вариантов более подробно.

1)Аренда выделенного канала и подключение к ЦОД для доступа к облаку

В настоящее время очень популярен вариант соединения внутренней сети заказчика с сетью в облаке IaaS-провайдера. Такой сценарий часто именуют гибридным облаком, так как заказчик имеет свои собственные ресурсы, а площадка IaaS-провайдер предоставляет только дополнительную вычислительную мощность. На физическом уровне данное решение представляет собой использование двух выделенных каналов провайдера, работающих в режиме автоматического переключения в случае падения одного из них. Как правило, такой канал связи предоставляется на основе собственной

оптоволоконной сети провайдера с возможностью подписания соглашения об уровне обслуживания, регламентирующего гарантии соблюдения технических характеристик канала. Несомненным плюсом данного метода является в его относительная дешевизна по сравнению с вариантом, когда заказчик пробрасывал бы свой собственный кабель. При этом провайдер, как правило, дает гарантию высокой плотности покрытия, а также безопасности и надежности арендуемых каналов, включая возможность резерва емкости при росте канала.

2)Проброс своего кабеля до ЦОД

Внутренняя сеть заказчика и сеть в облаке IaaS-провайдера также могут быть соединены пробросом собственного кабеля клиента до необходимого центра обработки данных. Такой метод является менее экономичным, по сравнению с предыдущим. Поэтому компании, которые нуждаются в высокоскоростных телекоммуникационных каналах, в большинстве случаев предпочли бы ранее рассмотренный нами вариант: аренду каналов или выкуп оптических волокон в уже проложенной линии связи. Однако организации, предъявляющие повышенные требования к безопасности и эксплуатационным показателям канала связи вынуждены сделать выбор в пользу прокладки собственной оптической линии.

3)Использование точек обмена трафиком

Этот способ прокладывания канала от организации к IaaS-провайдеру является удешевленной версией метода, рассмотренного ранее. Его суть заключается в том, что кабель прокладывается не до центра обработки данных облачного провайдера напрямую, а до коммутационного оборудования, размещенного IaaS-провайдером на площадках, где располагаются точки обмена трафиком. Точка обмена трафиком — это место, где осуществляется прямой обмен трафиком между интернет-операторами, минуя сети сторонних провайдеров. Все ее участники имеют возможность построить соединения друг с другом, задействовав при этом лишь один порт. Благодаря прямым пирингам,

через точку обмена можно в разы уменьшить загрузку внешних каналов и сократить время передачи данных между участниками. Для безопасной обработки данных обязательным условием является их шифруемая передача. В целях защиты данных в публичном облаке используется туннель виртуальной частной сети (VPN), связывающей клиента и сервер для получения публичных облачных услуг. 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).

Большинство протоколов SSL и VPN в качестве опции поддерживают использование цифровых сертификатов для аутентификации, посредством которых проверяется идентификационная информация другой стороны, причем еще до начала передачи данных. Такие цифровые сертификаты могут храниться на виртуальных жестких дисках в зашифрованном виде, и используются они только после того, как сервер управления ключами проверит идентификационную информацию и целостность системы. Следовательно, такая цепочка взаимозависимостей позволит передавать данные только тем облачным серверам, которые прошли предварительную проверку[15].

Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения в них, даже в случае доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, IPsec давно используются провайдерами.

2.2.2 Аутентификация

Решение проблемы безопасности пользователя в облачных вычислениях часто зависит от выбранных механизмов аутентификации. Самым популярным методом решения до сих пор является пароль. Большинство клиентов выбирают для пароля слова, которые легче запомнить, имена и номера

телефонов. Для получения подобного пароля злоумышленнику достаточно совершить перебор по словарю.

Альтернативой данного метода защиты считается двухфакторная аутентификация. На данный момент наиболее распространена технология двухфакторной аутентификации, использующая, одноразовые пароли (One Time password). Такие пароли могут генерироваться либо специальными программами, либо дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS и действуют в течение ограниченного времени. Суть этого метода — пароль действителен только для одного входа в систему, при каждом следующем запросе доступа требуется новый пароль. В настоящее время существует несколько реализаций технологии одноразовых паролей. Для ее использования могут применяться такие средства, как:

— Виртуальные токены (Mobile-OTP);

— Аппаратных токены (Aladdin eToken PASS);

— Аутентификация через SMS (RSA Mobile);

— Аутентификация One Time Matrix (OTM).

Рассмотрим подробнее каждый из способов реализации технологии одноразовых паролей.

1) Принцип работы виртуальных токенов.

На устройство пользователя устанавливается специальное приложение – программный токен. Он работает на принципе двухфакторной аутентификации. После установки приложения, пользователю необходимо пройти процесс регистрации своего устройства на сервере организации, к ресурсам которой требуется осуществить доступ. Далее для генерирования одноразового пароля пользователю необходимо ввести PIN код в приложении на своем устройстве. Полученный одноразовый пароль пользователь может использовать для входа в систему.

2) Принцип работы аппаратных токенов.

Как правило аппаратный токен представляет собой компактное устройство, предназначенное для идентификации его владельца и упрощения аутентификации. Для генерирования одноразового пароля должна существовать синхронизация между токеном клиента и сервером аутентификации. Основными недостатками токенов этого типа являются ограниченный срок службы, возможность рассинхронизации и утери.

3) Принцип работы технологии аутентификации через SMS.

Основное отличие облачной инфраструктуры заключается в том, что доступ пользователя в систему не должен быть территориально ограничен. Именно поэтому на первый план выходит использование мобильных устройств для получения одноразовых паролей, которые сегодня есть в наличии практически у каждого. 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. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language). Плюсом данного метода аутентификации является замена токена или любого другого аналогичного устройства текстовым SMS-сообщением, которое приходит на ваш мобильный телефон, снимая необходимость закупки, поддержки и замены вышедших из строя токенов.

4) Принцип работы технологии аутентификации One Time Matrix.

Одноразовая матрица (One-Time Matrix, OTM) — это разновидность технологии одноразовых паролей, которая не требует никаких дополнительных устройств для использования. В основе технологии доступа OTM лежит использование одноразового пароля, который формируется путем распознавания заданного шаблона (матрицы) и последовательного считывания цифр, отображенных в ячейках шаблона. Под шаблоном понимается

последовательность произвольно выбранных пользователем ячеек одноразовой матрицы, которую пользователь должен сохранить в системе, и используемая в качестве эталонного аутентификатора. Набор цифр в ячейках матрицы генерируется случайным образом при каждой попытке аутентификации, что исключает возможность повторного использования одного и того же кода доступа.

Наиболее перспективной на данный момент является технология биометрической аутентификации. Это форма аутентификации, в которой физиологические черты человека используются для идентификации или проверки подлинности пользователя. На данный момент биометрическая аутентификация еще не получила должного распространения в связи с технологической сложностью системы.

2.2.3 Шифрование

Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в центрах обработки данных, а также в случае отсутствия необходимости, безвозвратно удалять. При шифровании данных самым важным вопросом является месторасположение ключей. Их хранение на облачном сервере является бессмысленным, поскольку каждый, кто имеет доступ к облачным серверам или шаблонам, может получить доступ к ключу и расшифровать данным. Набор пароля при запуске системы, как это принято в локальных решениях для шифрования данных, невозможен в связи с отсутствием консоли ввода. Поэтому физический ввод ключа заменяется запросом, который облачный сервер отправляет внешнему источнику — серверу управления ключами (Key Management Server, KMS). Решающим фактором для обеспечения безопасности такого решения является раздельная эксплуатация облачного сервера и сервера управления ключами: если оба размещены у (одного и того же) провайдера облачных сервисов, то вся

информация оказывается собранной в одном месте. Хорошей альтернативой является установка сервера KMS в локальном ЦОД или в качестве внешней услуги у другого сервис-провайдера[16].

2.2.4 Изоляция пользователей

При использовании облачных вычислений периметр сети компании может размыться или и вовсе исчезнуть. Это приводит к тому, что защита каждого отдельного пользователя определяет общий уровень защищенности. Но важно не только предоставить пользователям безопасный способ обработки данных, но и защитить информацию. В том числе и от инсайдеров. Корпоративный firewall — основной компонент для внедрения политики IT безопасности и разграничения сегментов сети, не в состоянии повлиять на серверы, размещенные в облачных средах. Поэтому важно, чтобы виртуальные сети были развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service)[17].

Также провайдеры могут изолировать 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. В последнее время такие инциденты часто имели место.

Безопасность не всегда обеспечивается только защитой. Она может быть достигнута также соответствующими организационными правилами поведения и взаимодействия объектов и высокой профессиональной подготовкой персонала. Конфиденциальность информации – это принцип аудита, заключающийся в том, что аудиторы обязаны обеспечивать сохранность документов, получаемых или составляемых ими в ходе аудиторской деятельности, и не вправе передавать эти документы или их копии каким бы то

ни было третьим лицам, либо разглашать устно, содержащиеся в них сведения без согласия собственника экономического субъекта. За исключением случаев, предусмотренных законодательными актами.

3 Выбор оптимальных методов защиты облачных ресурсов

3.1 Сравнения облачных технологий

Так как клиенты часто не интересуются степенью ответственности поставщика за предоставляемые ресурсы, первым этапом является выбор облачного сервиса, наиболее подходящего критериям потребителя. В настоящее время существует множество как платных, так и бесплатных облачных сервисов, предоставляющих разные наборы услуг. Выбор облачной инфраструктуры в первую очередь зависит от нужд клиентов. Поэтому, организации или частному лицу в первую очередь необходимо определиться с моделью обслуживания. Как уже упоминалось ранее, существует три основных вида моделей IaaS, PaaS и SaaS.

Если компании необходимы дополнительные вычислительные мощности и нет возможности покупки дополнительных серверных машин, то наиболее удачным решением является выбор IaaS модели. На данный момент этот тип услуги предлагают такие провайдеры, как IBM SmartCloud Enterprise, VMWare, Amazon EC2, Windows Azure, Google Cloud Storage, Parallels Cloud Server и многие другие. Но так немногие компании согласятся доверить свои данные серверам, расположенным в других странах, первым критерием стало территориальное расположение дата-центров.

Безусловным лидером виртуализации серверных ресурсов для корпоративного сегмента сегодня является VMware, благодаря функции «High Availability», поддержке требуемых ОС, возможности по сопряжению с собственной виртуальной инфраструктурой и возможности использования функциональности SRM[18]. Поэтому здесь будут рассмотрены только провайдеры, поддерживающие эту технологию виртуализации. Сравнительный анализ российских провайдеров приведен в таблице 1.

Таблица 1

Сравнительная стоимость HDD у российских провайдеров

	Провайдер IaaS	Системы хранения данных	Стоимость HDD при статической модели, руб/мес	Стоимость HDD при динамической модели, руб/мес
1	IT-GRAD	NetApp FAS 6240	30	44
2	Dataline	NetApp FAS 6210, HP MSA P2000	20	40
3	Cloudone	NetApp FAS 2040, NetApp FAS 3240	14	нет
4	ONLANTA	HDS HUS	32	нет
5	SafeData	NetApp FAS 3250	24	30
6	Cloud4Y	NetApp FAS 3250	38	нет
7	Croc	EMC VNX 5700	26	40
8	I-Teco	3PAR 10400, IBM Storewize 7000, IBM XIV	30	нет
9	MegaFon	HP EVA 8400	28	нет

10	RTComm-Sibir	EMC VNX	30	нет
11	SoftLine	NetApp FAS 2240	30	44
12	DEPO Electronics	NetApp E-series	26	нет

Из представленных вариантов невозможно выделить оптимальное решение, так как каждая компания индивидуально выбирает параметры, которым будет уделено наибольшее внимание.

Для организаций, занимающихся созданием нового программного обеспечения, могут потребоваться значительные вычислительные ресурсы, Но они не всегда заинтересованы в администрировании баз данных и операционных систем, так как необходимым является только ограниченный набор продуктов. В этом случае идеальным решением является модель PaaS. В настоящее время данная услуга предоставляется такими компаниями, как:

— IBM SmartCloud Application Services;

— Amazon Web Services;

— Windows Azure;

— Boomi;

— Cast Iron;

— Google App Engine и другие.

При выборе управляющей моделью компании следует опираться на такие критерии, как:

— Количество создаваемых приложений;

— Какой тип приложений разрешен;

— Базы данных какого типа поддерживаются;

— Поддерживается ли протокол SSL (HTTPS).

Ниже приведена сравнительная таблица PaaS платформ.

Таблица 2

Сравнение PaaS платформ

Платформа	Поддерживаемые языки програмирования	Поддерживаемые базы данных	Стоимость, $
Beanstalk	Java, .NET, PHP, Node.js, Python, Ruby, Go и Docker	Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB или Microsoft SQL Server, Oracle	от 0.05 до 4.10 за час
Force.com	HTML, CSS, and JavaScript	Oracle Database	75 за пользователя в месяц
Heroku	Ruby, Java, Node.js, Scala, Clojure, Python, Go и PHP	Cloudant (англ.), Membase (англ.), MongoDB и Redis[7], помимо основной — PostgreSQL	от 0.05 до $0.10 за час
Microsoft Azure	Java, PHP, Ruby, Node.js, C	SQL Server	от 0.02 до 0.64 за час
OpenShift	.NET Core 1.0 .NET Core 1.1 Node.js 0.10 Node.js 4 PHP 5.5 PHP 5.6 Python 2.7 Python 3.3 Python 3.4 Python 3.5 Ruby 2.0 Ruby 2.2 Ruby 2.3 Perl 5.16 Perl 5.20 Tomcat 7 Tomcat 8	MariaDB 10.1 MongoDB 2.4 MongoDB 2.6 MongoDB 3.2 MySQL 5.5 MySQL 5.6 PostgreSQL 9.2 PostgreSQL 9.4 PostgreSQL 9.5	от 0.02 до 0.10 за час
App Engine	Python, Java, Go, PHP	-	от 0.05 за час
Engine Yard	Ruby, JRuby, REE, Rubiniu, Node.js, PHP	MySQL и PostgreSQL	от 0.05 до 2.19 за час

Также существует решение, для конечных пользователей, у которых есть необходимость работы с конкретным приложением, которое по тем или иным причинам не может быть установлено на их рабочей станции или необходим удаленный доступ. Такие функции реализованы в модели SaaS. Примерами SaaS являются Gmail, Google Docs, Netflix, Photoshop.com, Acrobat.com, Intuit QuickBooks Online, IBM LotusLive, Unyte, Salesforce.com, Sugar CRM и WebEx. Значительная часть растущего рынка мобильных приложений также является реализацией SaaS.

В то время как использование таких сервисов как Gmail, Google Docs, Netflix, Photoshop.com зависит от конкретных целей пользователя и их сравнение не представляется возможным из-за выполнения совершенно различных функций, сравнение облачных хранилищ данных не имеет смысла из-за небольших различий, состоящих в цене и объеме предоставляемого места.

Именно этот тип инфраструктуры наиболее подвержен существованию вероятности завладения злоумышленником данных, а также поставщик наименее заинтересован в сохранении конфиденциальности хранимой или обрабатываемой информации пользователей или даже претендует на принадлежность ему всех полученных файлов. Для того чтобы пользователь смог безопасно хранить и передавать свои данные, он должен в первую очередь установить безопасное соединение с удаленным центром обработки данных.

3.2 Сравнительные характеристики типов подключения

Так как возможные атаки на сеть и маршрутизаторы непосредственно не учитываются поставщиком при построении облачной инфраструктуры, клиенты часто не являются достаточно компетентными в вопросах информационной безопасности или забывают о необходимости защиты своей сети.

Подобная неосведомленность клиентов о том, каким образом и через какие сетевые узлы проходят их запросы к распределенной системе облака,

создает возможность проникновения извне и является первой уязвимостью, подлежащей устранению. Особенно это актуально для компаний, имеющих в своем распоряжении только рабочие станции и использующих серверные ресурсы внешнего облака.

Для практической реализации методов защиты от угроз этого типа целесообразно применять межсетевой экран, а также шифровать канал передачи данных и проводить аутентификацию пользователей. Немаловажным фактором в то же время является разграничение прав доступа пользователей и контроль над равномерным распределением их полномочий в порядках установленного регламента. При этом основной проблемой остается поиск подобных средств защиты, адаптированных под условия работы в облачной инфраструктуре. Для выбора наиболее подходящего типа подключения была составлена сравнительная таблица (Приложение 1).

Выбор конечного решения зависит от того, какая именно модель обслуживания является для пользователя наиболее актуальной и соотносится с предоставляемыми провайдером услугами. Практически любой из предложенных методов способен обеспечить безопасную передачу данных потребителя облачных сервисов. Однако любой из этих типов подключения не является гарантией того, что данные не будут изменены и похищены непосредственно из облачной системы. Для того чтобы полностью обезопасить свои данные рекомендуется также дополнительно шифровать файлы.

3.3 Выбор облачного сервиса для тестирования

Хотя в настоящее время многие облачные сервисы защищают информацию пользователя от проникновения извне, важно также обеспечить безопасность и от сотрудников компании провайдера. Особенно это важно при использовании приложений хранения данных. Поэтому к облачным сервисам, на которых будут тестироваться способы шифрования, были выдвинуты следующие требования:

— Доступ клиента осуществляется по модели частное облако;

— Это должен быть облачный сервис хранения данных, так как это наиболее запрашиваемое приложение на данный момент;

— Облачный клиент должен находиться в свободном доступе.

Среди всех представленных на рынке вариантах был выбран ownCloud. Преимуществами данного приложения являются возможность бесплатного использования для частных пользователей, клиенты синхронизации данных под управлением Windows, OS X или Linux и с мобильными устройствами на iOS и Android, возможность редактирования текстовых файлов и множество дополнительных функций (календарь, адресная книга, фотогалерея и т.д.)[19].

Для установки облачного сервиса хранения данных на базе НИИ Масштаб был поднят сервер под управлением ОС Ubuntu Server 14.04 и проложено VPN соединение типа Remote access (Рисунок 2).

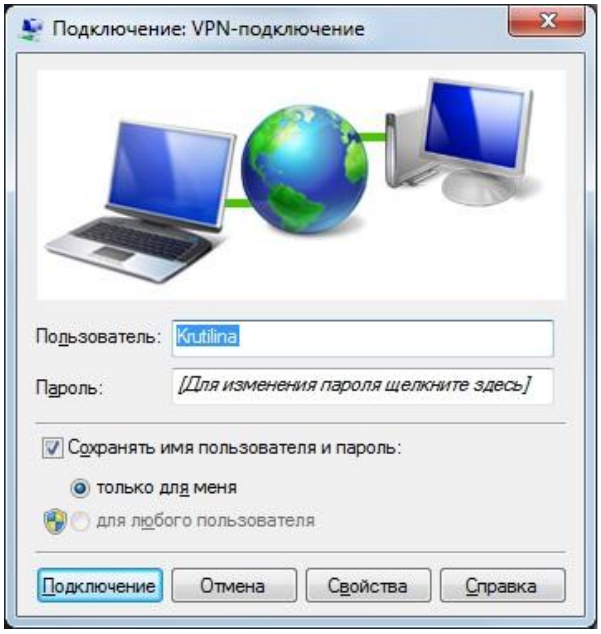

Рисунок 2 – VPN подключение к серверу

Для удаленного доступа к серверу был использован свободно распространяемый клиент PuTTY (Рисунок 3). Данное приложение позволяет подключиться и управлять удаленным сервером (Рисунок 4), используя такие протоколы, как SSH, Telnet, rlogin.

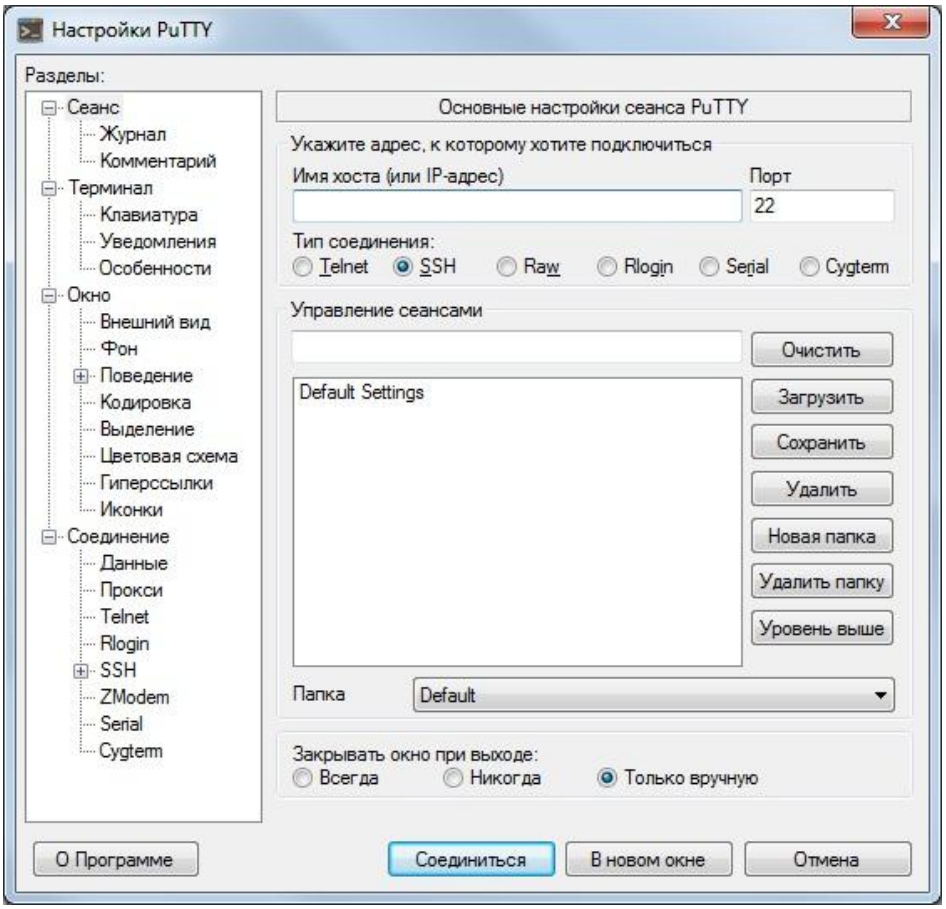

Рисунок 3 – Интерфейс клиента PuTTY для подключения к серверу

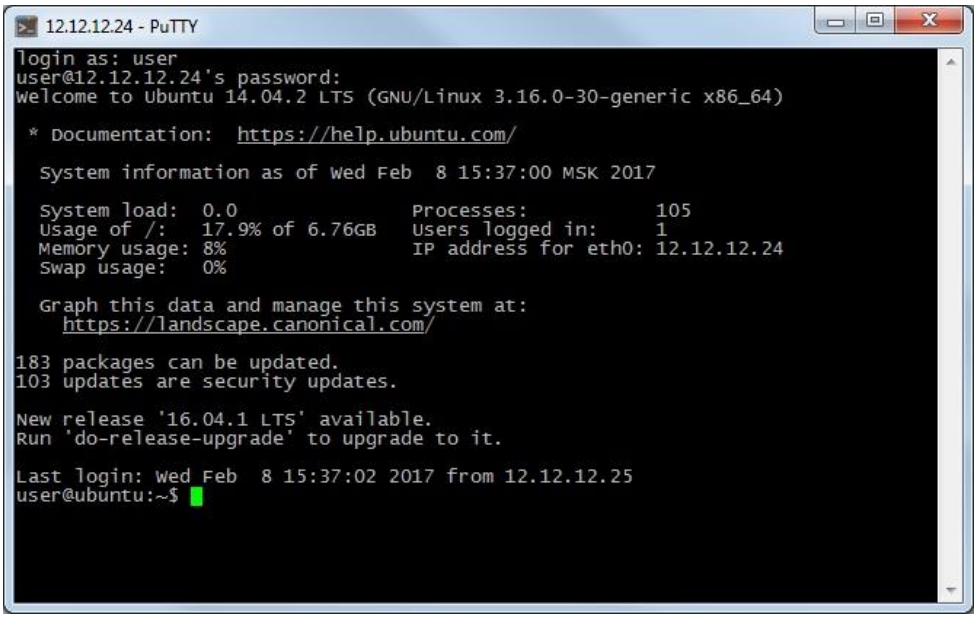

Рисунок 4 – Вид сервера

Чтобы установить ownCloud на сервер были установлены пакеты свободной реляционной системы управления базами данных MySQL 5.5, а

также модули веб-сервера Apache 2.2 и PHP5. После этого из интернета был скачан установщик ownCloud и установлен на сервер.

Для того чтобы зайти в облачное хранилище необходимо ввести в браузере адрес http://ip_адрес_пользователя/owncloud. Вид облачного хранилища на сервере указан на данном рисунке:

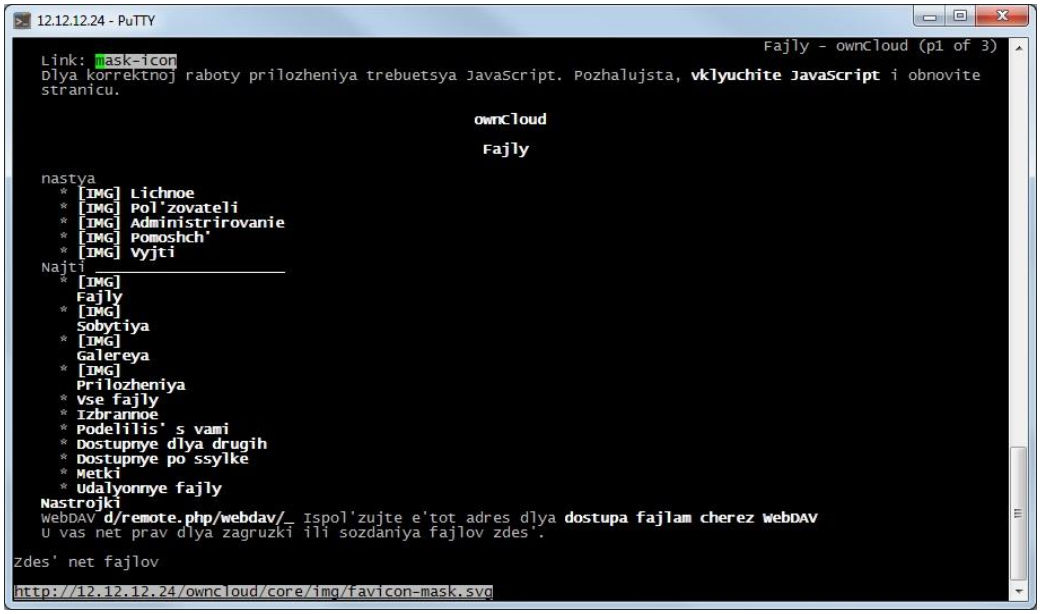

Рисунок 5 – Вид облачного хранилища на сервере

А здесь приведено отображение хранилища в браузере:

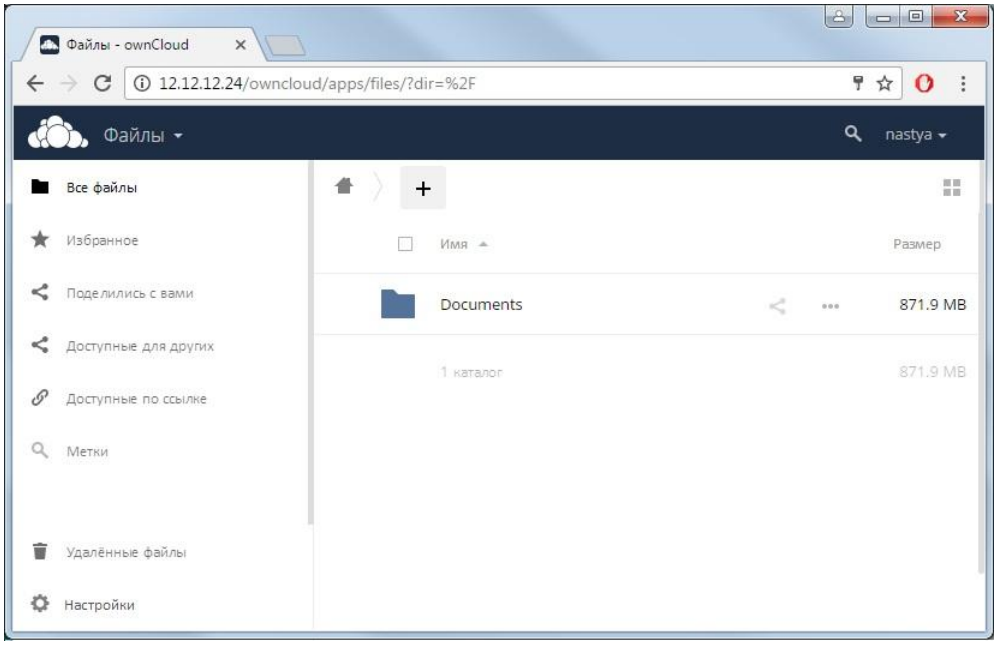

Рисунок 6 – Вид облачного хранилища в окне браузера

3.4 Выбор метода шифрования

Безопасность передачи и хранения файлов сейчас имеет очень большое значение для любого пользователя сети Интернет. Именно поэтому важно обеспечивать дополнительную защиту данных. Одним из наиболее распространенных методов защиты является шифрование.

Для выбора метода шифрования применялись такие начальные критерии, как:

— Осуществляемо для Windows ОС;

— Облачный клиент не умеет синхронизировать файлы поблочно;

— Метод шифрования должен обеспечить возможность быстрого доступа к любому файлу на облаке для его обновления или дешифровки без необходимости передачи больших объемов паразитных данных.

Исходя из этих, условий было выделено несколько возможных методов шифрования:

1) Проприетарные программы, позиционируемые как средство для шифрования данных в облаке.

Особенность работы данных программ в том, что они шифруют отдельные файлы, представленные на диске, а потом с помощью библиотек Dokan или Eldos CBFS создают их виртуальное расшифрованное представление. При локальной работе файлы прозрачно расшифровываются, а при синхронизации папки пользователя с облачным хранилищем передаются в зашифрованном виде. Данные программы идеально подходят для пользователей, не имеющих опыта в шифровании данных.

Из существующих на данный момент программ была выбрана бесплатно распространяемая программа Boxcryptor (Рисунок 7). Boxcryptor является кросс-платформенной программой для персональных компьютеров и телефонов и поддерживает все наиболее популярные облачные хранилища данных. С ее помощью можно осуществить шифрование документов с помощью RSA и

симметричного алгоритма блочного шифрования AES с длинной ключа 256 бит.

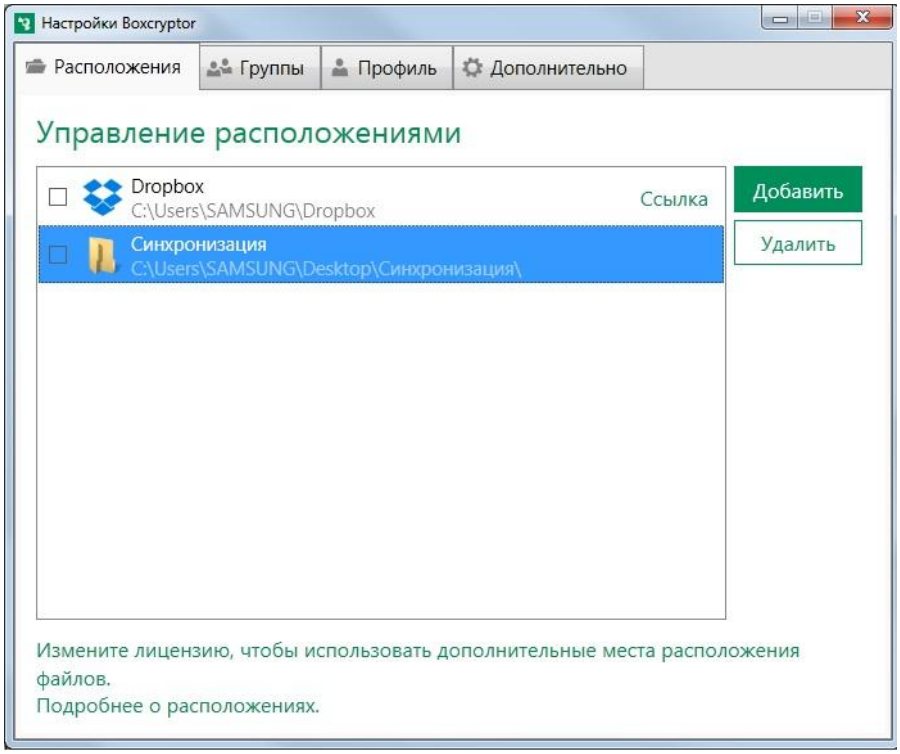

Рисунок 7 – Выбор синхронизированной папки для защиты

Недостатки данного подхода:

— Ограниченное количество функций в бесплатной версии программы;

— При утере пароля доступ к зашифрованным файлам становится невозможен и необходимо обратиться к администратору;

— Зашифрованные файлы можно просматривать только через интерфейс программы;

— В бесплатной версии можно загружать только один файл за раз;

— Субъективное мнение: недостаточная производительность, особенно при редактировании видео.

2) Порт EncFC для Windows

EncFL – это криптографическая файловая система, прозрачно шифрующая файлы, используя произвольную директорию в качестве места для хранения файлов. EncFS взаимодействует непосредственно с libfuse (интерфейс

FUSE), библиотекой логирования и OpenSSL (библиотека шифрования). Основная реализация системы поддерживается операционными системами Linux, Mac OS X, FreeBSD, но в последнее время получили активное развитие несколько реализаций под Windows[20].

EncFS имеет ряд преимуществ над другими системами шифрования разделов жёсткого диска, потому что каждый файл отдельно шифруется и сохраняется как обычный файл:

— Занимаемое EncFS дисковое пространство может расти и уменьшается в зависимости от изменений количества и размера зашифрованных файлов;

— Некоторые директории в директории-точке монтирования могут физически находиться на различных устройствах;

— Средства резервного копирования могут обновлять только те файлы, которые изменились в исходной директории, а не всю директорию;

— Это свободная система, с открытым исходным кодом;

— encf4win поддерживает ключ –reverse (Рисунок 8). В reverse-режиме локальные данные остаются нетронутыми, а шифруется только их отображение на виртуальном диске. Для работы encfs4win требуется установка библиотеки Dokan 0.6.0 (программного интерфейса для Windows, позволяющего создавать виртуальную файловую систему).

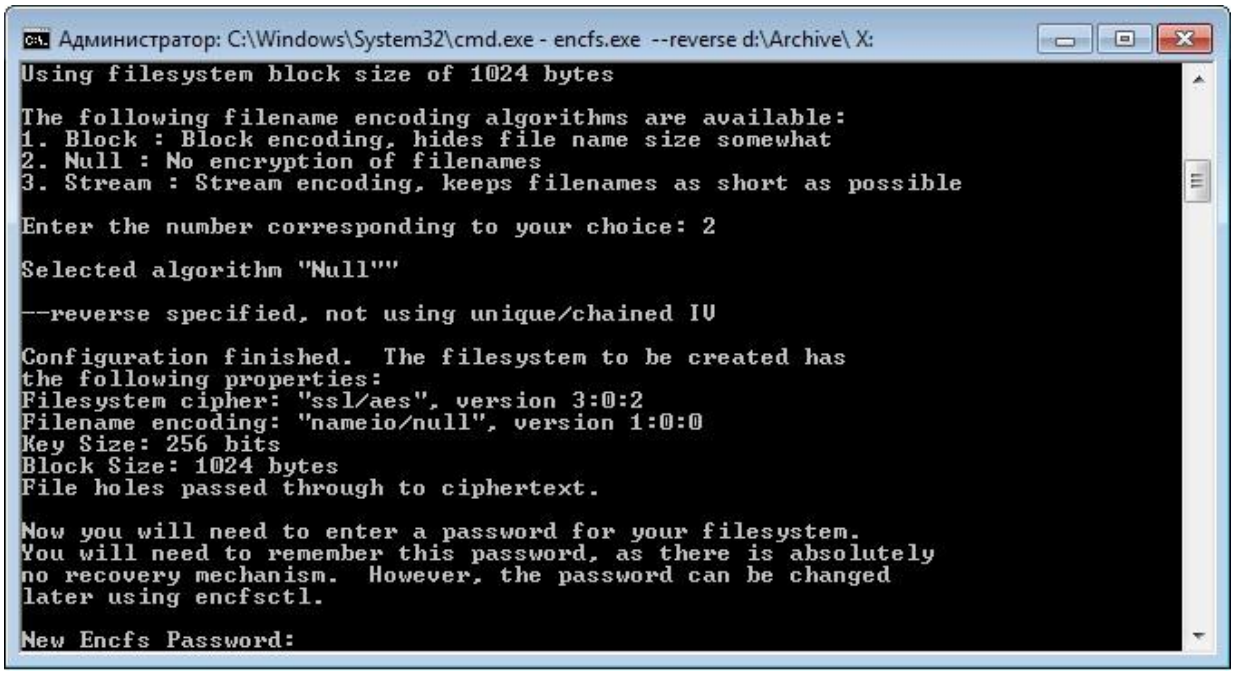

Рисунок 8 – Описание Reserve ключа

Недостатки подхода:

— Тома EncFS не могут быть отформатированы под произвольную файловую систему. Они сохраняют особенности и ограничения файловой системы, содержащей директорию-источник;

— Фрагментация зашифрованного тома вызывает фрагментацию файловой системы, содержащей директорию-источник;

— Каждый пользователь, имеющий доступ к директории-источнику, способен видеть количество файлов в зашифрованной файловой системе, какие права они имеют, их приблизительный размер, приблизительную длину имени и дату последнего доступа или изменения.

3) Локальное шифрование файлов в архивы, защищенные паролем, и их последующая синхронизация с облаком. Утилита CryptSync.

CryptSync — это программа, которая синхронизирует две папки и шифрует одну из них, поэтому в распоряжении пользователя оказываются как непосредственно файлы, с которыми предстоит работать, так и их безопасная резервная копия. Открытая исходная программа шифрует папки с использованием формата 7-Zip, поэтому пользователь получает не только

зашифрованные, но и уменьшенные в объеме данные (Рисунок 9). Данная программа не только индивидуально шифрует каждый файл, и его название.

С помощью CryptSync также возможно шифрование и копирование файлов с компьютера на ноутбук или же с компьютера на внешний источник.

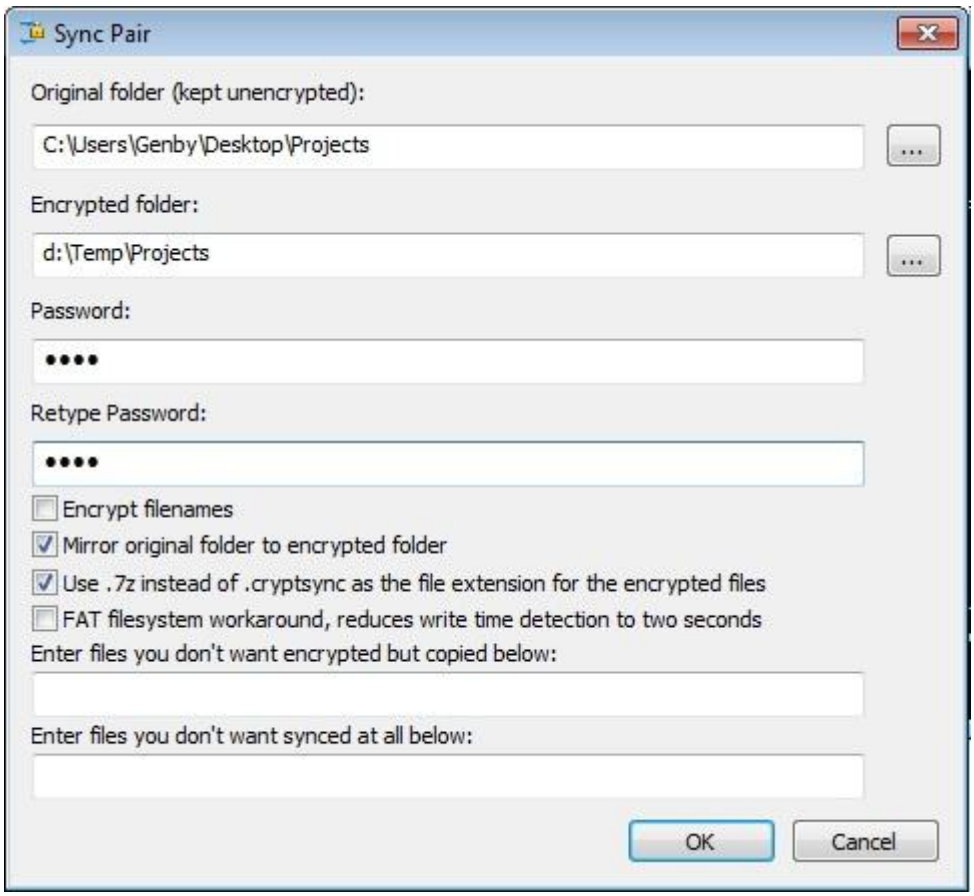

Рисунок 9 – Выбор шифруемой папки

Недостатки:

— Единственная поддерживаемая платформа — Windows;

— Необходимо хранить две копии файлов на локальном диске;

— Имеет недостаточный уровень защищенности, по сравнению с другими мерами.

Приведенные выше решения предоставляют только зашифрованное представление данных в локальной папке пользователя. Дальнейшая синхронизация может осуществляться любимым webdav-клиентом, либо

официальным клиентом облака. Представленные же ниже варианты имеют автоматическую интеграцию с облачными сервисами.

4) Duplicati

Duplicati — это программа с открытым исходном кодом, предназначенная для резервного копирования и созданная на основе одноименной утилиты с платформы Linux. Основной особенностью этой программы является возможность создания полноценного пошагового резервного копирования данных непосредственно в облако (Рисунок 10). Данной функцией поддерживаются такие облачные сервисы как, Google Drive, Skydrive, Amazon S3, Rackspace, Webdav, SFTP, FTP. На выбор предлагается шифрование встроенной библиотекой SharpAESCrypt (алгоритм шифрования AES-256) или средствами GnuPG (приложение для защиты сообщений и файлов, использующее шифрование и электронную цифровую подпись).

Среди многочисленных функций Duplicati особенный интерес также вызывает возможность быстрого восстановления отдельного файла из облака. Резервные копии при создании автоматически разбиваются на блоки размером 10 Мбайт. Поэтому при восстановлении одиночного файла будет задействовано ограниченное количество блоков. Помимо этого данная программа полностью конфигурируема через командную строку и поддерживает портативный режим[21].

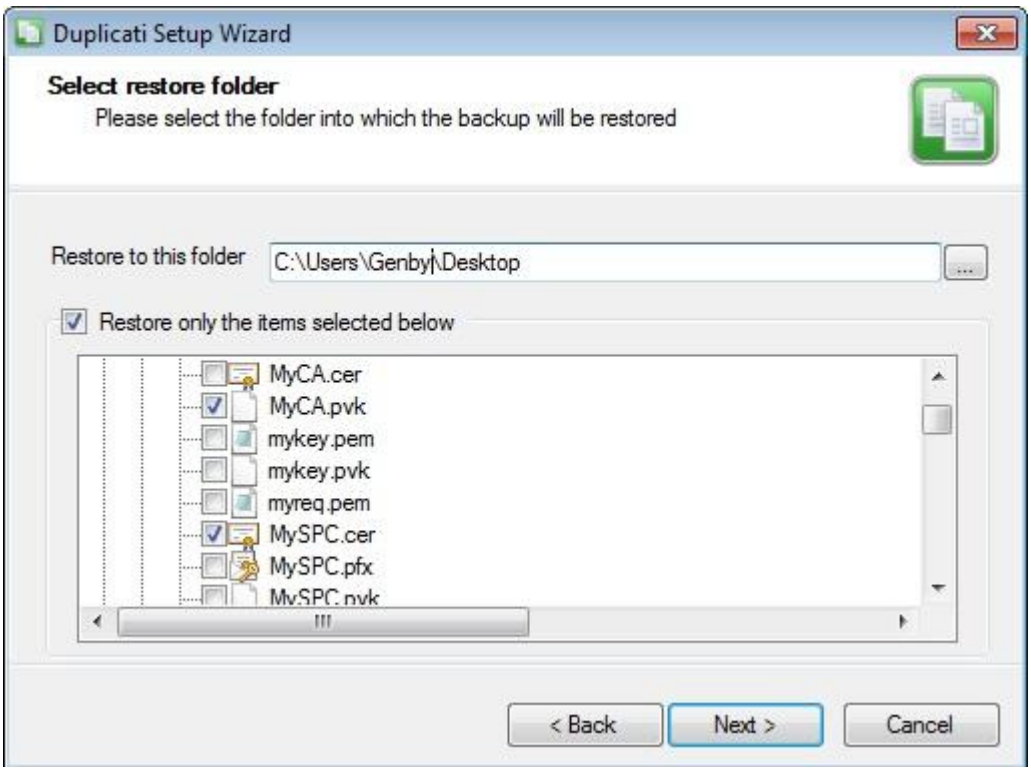

Рисунок 10 – Выбор папки для резервного копирования

Недостатки использования Duplicati:

— Невозможность обновления отдельного файла на облаке, кроме как путём создания новой инкрементальной итерации всего архива;

— Неудобно и долго восстанавливать одиночные файлы посредством использования графического интерфейса пользователя, особенно после нескольких инкрементальных итераций и при большом размере блока;

— Все данные о подключениях к облачным сервисам сохраняются в базе данных Sqllite, зашифрованной стандартным паролем.

5) Клиент CarotDav.

CarotDAV – это программа, которая помогает организовать удобный доступ, загрузку и управление файлами в нескольких облачных сервисах одновременно (Рисунок 11). Данный клиент не предоставляет всех функций, которые поддерживают фирменные клиенты облачных хранилищ данных, но может быть удобен в случае необходимости единовременного использования нескольких сервисов, например во время передачи файлов между ними. Кроме

webdav-облаков CarotDAV осуществляется поддержка таких облачных платформ, как SkyDrive, Dropbox, GoogleDrive, Box, SugarSync и FTP(S). Данная программа написана на объектно-ориентированном языке программирования VB.NET и является полностью свободной для использования и модификации. Из отличительных особенностей также можно выделить наличие портативного режима и защиту конфигурации мастер-паролем[22].

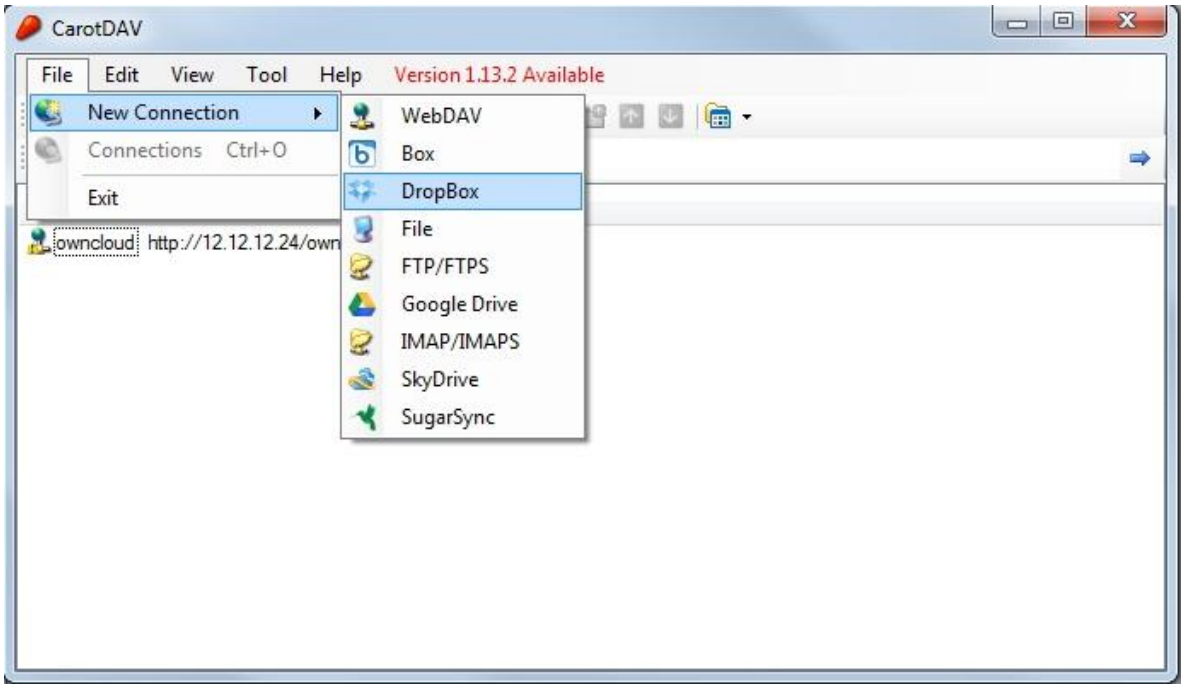

Рисунок 11 –Интерфейс программы CarotDAV

Недостатки:

— Возможны ошибки при работе с некоторым webdav облаками, которые можно решить увеличением времени ожидания соединения;

— Иногда возникают проблемы с поддержкой русского языка;

— Неудобный графический интерфейс пользователя и отсутствие управления через командную строку.

3.5 Экономическое обоснование

Самой большой проблемой для руководителей компаний и IT-специалистов являются целесообразность перехода на облачную платформу и

оценка экономических выгод и рисков от внедрения облачных вычислений. Оценка экономической эффективности является необходимым компонентом любого технико-экономического обоснования ИТ-проекта. Это увеличивает важность вопросов по выбору методики по оценке эффективности и рисков от внедрения ИТ[23].

В современных условиях в области внедрения облачных технологий остро стоит проблема недостаточной проработанности комплексной методологической основы и инструментальной среды поддержки принятия решений, основанная на процессах оценки эффективности и рисков в условиях неопределенности среды принятия решений. Эта проблема является актуальной для организаций любого размера и отрасли.

Первым этапом решения проблемы является определение затрат и выгод при переходе к облачным сервисам. На этапе определения высокоуровневых требований бизнеса необходимо выявить[24]:

— Функции бизнеса;

— Причины перевода бизнеса на облачные сервисы;

— Облачные сервисы, которые могли бы поддерживать бизнес-процессы;

— Правовые требования;

— Определение места, в котором будут размещены системы, обеспечивающие предоставление услуг и кто будет отвечать за предоставление услуг.

Следующим шагом является определение базовой модели облачного сервиса с точки зрения риска. Здесь определяются области риска, которые необходимо принять в расчет и меры по снижению риска в выявленных областях до приемлемого уровня с точки зрения предприятия. Далее определяется, какой тип облачной модели (SaaS, PaaS, IaaS) нужен предприятию, а также какова модель размещения облака (публичное, частное, общественное, гибридное) лучше всего подойдёт компании.

Предварительный анализ издержек включает в себя:

— Стоимость перенонoса существующей модели в облачную систему;

— Стоимость работы с облачной моделью;

— Единовременные и постоянные затраты на средства снижения рисков.

На втором этапе производится оценка рисков существующей модели: описывается модель, которая используется в настоящее время для оказания услуг в соответствии с функциональными и правовыми требованиями бизнеса.

В оценке рисков для существующей модели предоставления услуг определяются:

— Области, в которых риск превышает приемлемый для предприятия уровень;

— Меры, которые помогут снизить риск до приемлемого уровня;

— Области риска, которые существуют для текущей технологии, чтобы убедиться, что в оценке существующего и будущего состояния руководствовались одним и тем же.

— Третий этап состоит в определении планируемого периода использования облачных и производится расчёт критериев и показателей эффективности и рисков по предложенным моделям.

— Далее необходимо сравнить существующее и желаемое состояния:

— Определить числовые показатели для прямых выгод;

— Рассчитать перехода в облако сервис;

— Сопоставить показатели затрат и выгод для существующего и желаемого состояния.

— Рассчитать себестоимость и прибыль за каждый год.

Расчет критериев и коэффициента «Эффективность облачного сервиса» проводится по аддитивной формуле:

$$Kecs = \left(\sum_{1}^{6} a1 \times \text{П}I\right) \times 100\%$$

$$Kecs = (a1 \times \text{Эб} + a2 \times \text{Фп} + a3 \times \text{Тп} + a4 \times \text{Иб} + a5 \times \text{Ср} + a6 \times \text{Пф}) \times 100\%$$

где Kecs – критерий «Effectiveness of cloud-based services»;

Эб – значение критерия «Эффективность для бизнеса»;

Фп – значение критерия «Финансовые преимущества»;

Тп – значение критерия «Технический приоритет»;

Иб – значение критерия «Надежность работы и информационная безопасность»;

Ср – значение критерия «Степень риска использования облачного сервиса»;

Пф – значение критерия «Психологический фактор».

a1, a2, a3, a4, a5 – коэффициенты степени влияния.

Алгоритм расчета критериев эффективности:

1. Сравнение с требуемыми показателями и стандартами, исходя из ответов провайдера облачного ИТ-сервиса. Главным принципом сравнения является принцип обеспечения сопоставимости результатов на основе принятой шкалы экспертных оценок.

Таблица 3

Шкала предпочтительности показателей

Значение показателя	Вербальное значение показателя эффективности облачного сервиса
1	Показатель эффективности применения облачного сервиса очень высокий
1,00…0,75	Показатель эффективности довольно высокий
0,75…0,5	Показатель эффективности вроде бы высокий
0,5	Средний уровень показателя эффективности
0,5…0,25	Показатель эффективности вроде бы низкий
0,25…0	Показатель эффективности довольно низкий
0	Показатель эффективности очень низкий

2. Бальная оценка экспертом степени соответствия требованиям безопасности облачных вычислений в соответствии со шкалой. Для назначения баллов используется десятичная шкала от 0 до 1.

3. Расчет критерия по формуле.

Главной особенностью принятия решений на внедрение облачных технологий является то, что они принимаются в условиях высокой неопределенности среды. Также важно понимать, что технико-экономические расчеты носят ориентировочный характер. Их стоит проводить, если ваша задача – обосновать целесообразность модернизации ИТ-инфраструктуры на конкретном объекте и выбрать наиболее эффективный, в том числе и с экономических позиций, вариант реализации данной инфраструктуры из числа возможных альтернатив[26]. При неполноте и невысоком качестве исходной информации лицо, принимающее решение, вынуждено отклониться от точных числовых оценок, заменяя качественными характеристиками.

К сожалению, все еще не существует идеального метода защиты данных, доступных для рядового потребителя облачных сервисов. В каждом из рассмотренных вариантов предоставления облачных услуг существуют свои особенности, способные привлечь пользователей и отвечать их поставленным задачам. Но, так как облачные услуги появились сравнительно недавно, можно ожидать, что в скором времени появится больше вариантов решения данной проблемы.

4 Обеспечение безопасности жизнедеятельности

4.1 Основные положения безопасности жизнедеятельности

В настоящее время компьютеры стали неотъемлемой частью повседневной жизни людей, и количество времени, проведенного за их использованием, постоянно растет. Но внедрение компьютеров несет за собой как положительные, так и отрицательные моменты. С одной стороны, использование компьютеров способно обеспечить высокую эффективность производства за счет улучшения технологического процесса и увеличения производительности, а с другой стороны это влечет за собой увеличение нагрузки на работе в связи с активизацией производственной деятельности и специфическими условиями труда.

Компьютеры все чаще используются в офисах в качестве вспомогательного средства обработки информации, поэтому внедрение данных технологий в корне изменило характер работы служащих и требований к организации и охране труда.

Несоблюдение требований безопасности может привести к тому, что при работе за компьютером работник может чувствовать почувствовать себя плохо: появление головной боли и боли в глазах, человек быстро становится усталым и раздражительным. У некоторых людей нарушается сон, аппетит, ухудшается зрение, начинают болеть руки, шеи, нижняя часть спины и т.д. Также при ненормированной работе нередки случаи нервного истощения.

В Российской Федерации, вопросы, касающиеся организации и безопасности при работе на компьютере, регулируются:

— Трудовым кодексом;

— «Гигиеническими требованиями к персональным электронно-вычислительным машинам и организации работы» (СанПиН 2.2.2 / 2.4.1340-03);

— «Типовой инструкцией по охране труда при работе на персональном компьютере» (ТОИ Р-45-084-01).

В соответствии с СанПиН 2.2.2.542-96:. "Гигиенические требования к ВДТ и ПЭВМ. Организация работы" все опасности, связанные с ВДТ и ПЭВМ можно разделить на три группы:

1) Параметры рабочего пространства и рабочей зоны;
2) Визуальные факторы (яркость, контрастность, мерцание, блики);
3) Излучение (рентгеновское, электромагнитное излучение, гамма-излучение, электростатическое поле).

Рабочие условия характеризуются способностью воздействовать на людей следующими производственными факторами:

— шумом,

— выбросами тепла,

— выбросами вредных веществ,

— статическим электричеством,

— ионизирующими и неионизирующими излучениями,

— низким уровнем света,

— параметрами технологического оборудования и рабочего места.

Основной опасностью для здоровья пользователя (и людей, находящихся в непосредственной близости от компьютера) является электромагнитное излучение в диапазоне 20 – 400 кГц, порожденное отклоняющей системой кинескопа и видеомонитора[27]. Многочисленные экспериментальные данные, свидетельствуют о влиянии ЭМП на живые организмы. В первую очередь это влияние распространяется на нервную, эндокринную, иммунную и кроветворную системы организма.

Наиболее опасной из всех является низкочастотная составляющая ЭМП (до 100 Гц), способствующая изменению биохимической реакции крови на

клеточном уровне. Это приводит к возникновению у человека симптомов раздражительности, нервного напряжения и стресса.

Видеомонитор создает вокруг себя ЭМП как низкой, так и высокой частоты, что способствует появлению электростатического поля и приводит к деионизации воздуха вокруг, а это влияет на развитие клеток тканей организма, увеличивает вероятность возникновения катаракты.

В качестве мер предосторожности обязательно следует использовать защитные экраны, а также рекомендуется ограничивать продолжительность работы с экраном ВДТ, не сосредотачивать их размещение в рабочей зоне и выключать их, если их не используют. Кроме того нужно устанавливать в помещении с ВДТ ионизаторы воздуха, часто проветривать помещение и по крайней мере один раз в течение рабочей смены выделять время, чтобы очистить экран от скопившейся пыли. Все ВДТ и ПЭВМ должны иметь техническую документацию и гигиенический сертификат.

4.2 Требования к параметрам воздушной среды

Воздух, поступающий в рабочее пространство операторов ЭВМ, обязан быть очищен от загрязнений, в том числе от примесей и вредных бактерий.

Кондиционирование воздуха должно обеспечивать поддержание параметров воздушного пространства в дозволенных пределах в течение всего года, а также очистку воздуха от пыли и вредных веществ, синтез необходимого избыточного давления в чистых помещениях для исключения поступления воздуха, непрошедшего обработку. Температура подаваемого воздуха обязана быть не ниже 19 градусов.

Следует также ограничивать количество вычислительной техники в помещении и избегать систем подогрева пола. Поверхность пола в помещениях должна быть, ровной, нескользкой, и такой, чтобы было удобной чистить и поводить влажную уборку. Покрытия рабочих столов и пола должны иметь

антистатические свойства и способность поддерживать их в процессе эксплуатации. В помещениях ежедневно должна проводиться влажная уборка.

4.3 Требования к уровню шума и вибрации

Основными источниками шума в помещениях, оснащенных вычислительной техникой, являются принтеры, плоттеры, копировальные аппараты и оборудование для кондиционирования воздуха, такие как вентиляторы систем охлаждения и трансформаторы. Уровень шума на рабочих местах не должен превышать 50 дБА. Нормируемые уровни шума обеспечиваются путем использования малошумного оборудования, применением звукопоглощающих материалов (специальные перфорированные панели, минераловатные плиты). Шумное оборудование, показатели которого превышают нормированные уровни шума, должно находиться вне помещения с компьютерами. Производственные отделения, в которых для работы применяютсяв основном персональные компьютеры, не должны находиться с помещениями, в которых уровни шума и вибрации превышают указанных значений[28].

4.4 Требования к освещению помещений и рабочих мест

Немаловажное место в комплексе мероприятий по созданию условий труда для сотрудников, трудящихся с ПЭВМ, занимает организация оптимальной светового окружения, т.е. рациональной организации естественного и искусственного освещения помещения и рабочих мест. Помещения, предназначенные для размещения рабочих мест пользователей персональных компьютеров, должны иметь доступ к естественному освещению, а также оборудованы средствами искусственного освещения.

Окна в помещениях, предназначенных для использования компьютеров, необходимо оборудовать устройствами контроля интенсивности естественного освещения типа жалюзи, занавесей или навесов.

Искусственное освещение в помещениях должно осуществляться единой системой равномерного освещения. В качестве источников местного освещения подойдут светильники, позволяющие избежать появления бликов и отражений, с возможностью регулирования пространственного положения, оснащенные рассеивателями светового потока и т.п. Свет в помещении, где происходит работа пользователей на персональных компьютерах, не должен создавать мерцаний бликов на экране и не увеличивать отражающих свойств экрана.

Для того чтобы обеспечить стандартизированные нормируемые значения освещенности в помещениях следует проводить очищение стекол в оконных рамах и светильников не реже двух раз в год, а также своевременно заменять перегоревшие лампы.

Так как при работе на компьютере существенная нагрузка приходится на глаза, больше внимания должно уделяться выполнению нормативов, предъявляемых к видеотерминальным устройствам (экранам). Наиболее предпочтительными оказываются плоские мониторы, с помощью которых можно избежать наличия ярких пятен за счет отражения световых потоков. Особенно важным является цвет экрана. Он должен быть нейтральным и изменяться в положенных пределах во время суток. Возможны ненасыщенные светло-зеленые, желто-зеленые, желто-оранжевые, желто-коричневые тона. При работе с ЭВМ взгляд должен падать на экран под прямым углом и угол отклонения от горизонтальной плоскости должен быть не больше чем 20градусов.

4.5 Требования к производственному оборудованию

Для того чтобы обеспечить электропитание компьютеров должна быть установлена отдельная сеть электропитания. Периферийное оборудование, подключаемое к компьютерам, также должно быть подключено только к линиям электроснабжения компьютерной сети[29].

Не допускается включение электроприборов, не связанных с компьютерами в линии электропитания компьютерной сети.

Не допускается использование оборудования с открытыми корпусами, если это не является основным режимом работы оборудования. Обслуживание оборудования рабочих мест должно производиться подготовленным персоналом, имеющим квалификацию инженера (техника), или специализированной организацией.

Электрические розетки системы электропитания должны быть расположены таким образом, чтобы электрические кабели оборудования, расположенные на рабочих местах, не затрудняли доступ к рабочему месту (были удалены от места расположения пользователя).

Рабочее место пользователя компьютера необходимо располагать по отношению к естественным источникам света таким образом, чтобы освещение находилось сбоку от пользователя. Рекомендуемое направление падения естественного света – слева от пользователя. Запрещено располагать места с размещенными пользователями таким образом, чтобы естественноеосвещение падало на них со стороны спины или лица работника.

При размещении рабочих мест с компьютерами необходимо учитывать расстояния между рабочими столами с электронными экранами, которое должно быть не менее 2,0 м, а расстояние между соседними гранямиэкранами – не менее 1,2 м.

Проемы между соседними местами должны иметь ширину, которая обеспечивает свободноепередвижение персонала без соприкасанияс оборудованием или материалами, расположенным на рабочем месте. Минимально необходимая ширина – 0,6 м, оптимальная - 0,9 м.

Рабочие места с компьютерами при выполнении творческой работы, которая требует больших умственных усилий или значительной концентрации внимания, следует изолировать друг от друга непрозрачными перегородками высотой 1,5-2,0 м.

Рекомендуется использование специализированных компьютерных столов в сочетании со столами для письменной работы. Высота рабочей поверхности стола должна иметь свойство регулироваться в пределах 680-800мм. При отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм. Рабочий стол должен иметь отделение для ног высотой не менее 600 мм, шириной не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Устройство рабочего стула должно обеспечивать поддержание удобной рабочей позы при работе на компьютере, позволять менять позу с целью уменьшения статического напряжения мышц опорно-двигательной системы и спины для предупреждения развития усталости.

Рабочее место должно быть оснащено подставкой для ног, имеющей ширину не менее– 300 мм, глубину не менее 400 мм, регулироваться по высоте в пределах до 150 мм и по углу наклона опорной плоскости подставки до 20 градусов. Пластина подставки должна быть ребристой и иметь по переднему краю бортик высотой 10 мм.

Монитор должен находиться от глаз пользователя на оптимальном расстоянии 600-700 мм, но не ближе 500 мм с учетом печатаемых знаков и символов.

Средства ввода информации (клавиатура, мышь) следует располагать на поверхности рабочего места на расстоянии 100-300 мм от края, направленного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной конструкции стола.

4.6 Режимы труда и отдыха при работе с компьютером

Режим труда и отдыха при работе с ПЭВМ и ВДТ должен организовываться в зависимости от вида и категории деятельности. Виды деятельности подразделяются на следующие группы:

— группа А - работа по считыванию информации с ВДТ или ПЭВМ с предварительным запросом;

— группа Б - работа по вводу информации;

— группа В - творческая работа в режиме диалога.

Для инженеров, обслуживающих учебный процесс в кабинетах (аудиториях) с персональными компьютерами, продолжительность работы не должна превышать 6 часов в день.

Для обеспечения наилучшей работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны быть нормативные перерывы. Время регламентированных перерывов в течение рабочей смены следует устанавливать в зависимости от ее длительности, вида и категории трудовой занятости.

Режим труда и отдыха пользователей, работающих с ЭВМ, должен быть следующим: через каждый час интенсивной работы необходимо устраивать 15 - минутный перерыв, при менее интенсивной, через каждые 2 часа. Эффективность регламентируемых перерывов повышается при их сочетании с производственными гимнастическими упражнениями.

Пользователи, использующие персональные компьютеры в качестве основного производственного средства, должны проходить обязательные предварительные (при поступлении на работу) и периодические медицинские осмотры в порядке и в сроки, установленные Минздравом России[30].

Местоположение рабочих мест пользователей персональных компьютеров в организациях в подвальных помещениях не допускается. В организациях площадь помещения, приходящаяся на одно рабочее место, оборудованное персональным компьютером, должна соответствовать требованиям технологической и эксплуатационной документации и составлять не менее 6,0 кв.м, а объем не менее 20,0 куб.м. Помещения должны быть оснащены аптечкой первой помощи и углекислотными огнетушителями.

Заключение

В настоящее время облачные средства вычисления получили активное распространение как среди организаций, нуждающихся в дополнительной вычислительной мощности, так и среди простых людей, желающих упростить процесс обработки и хранения данных. Но вместе с ростом пользователей увеличилось и количество выявленных уязвимостей этого метода обработки данных. Как и любые другие средства обработки данных, облачные сервисы имеют свои преимущества и недостатки.

Выделяют несколько преимуществ, связанных с использованием облачных технологий:

1. Доступность**.**

Доступ к информации, хранящейся в облачном сервисе, может получить любой человек, имеющий в своем распоряжении компьютер, планшет, либо любое мобильное устройство, подключенное к сети интернет.

2. Мобильность.

У пользователя нет постоянной привязанности к одному рабочему месту. Обработка информации может проводиться из любой точки мира со скоростью, равной скорости интернет-соединения пользователя.

3. Экономичность.

Одним из важных преимуществ является сниженная затратность использования облачных сервисов по сравнению со стандартными центрами обработки данных, так как в данном случае у пользователя нет необходимости в покупке дорогостоящих компьютеров и программного обеспечения, а также он освобождается от необходимости нанимать специалиста по обслуживанию локальных IT-технологий.

4. Аренда.

Пользователь имеет право получать только необходимые пакеты услуг с фактической оплатой потребляемой мощности и не переплачивать за ненужные функции.

5. Гибкость.

Все необходимые ресурсы предоставляются провайдером автоматически.

6. Высокая технологичность.

Провайдеры стремятся предоставить клиентам все большие вычислительные мощности, которые можно использовать для хранения, анализа и обработки данных. Поэтому данная отрасль активно развивается в настоящее время.

7. Надежность.

Некоторые эксперты утверждают, что надежность, которую обеспечивают современные облачные вычисления, гораздо выше, чем надежность локальных ресурсов, потому что только небольшое количество предприятий способно позволить себе полноценный центр обработки данных и обеспечить ему надлежащее содержание и безопасность.

Несмотря на все положительные отзывы, существует и определенная критика в адрес облачных технологий. Согласно исследованиям аналитической фирмы IDC, многие компании, в первую очередь, связывают с «облачными» сервисами большие проблемы по части безопасности. А независимая исследовательская организация Portio Research только подтвердила это, указав конкретные цифры: 68 % опрошенных руководителей европейских IT-компаний, в целях безопасности, отказываются использовать облачные технологии. Это связано с тем, что надёжность, своевременность получения и доступность данных, расположенных облачном хранилище, очень сильно зависит от многих промежуточных параметров, таких как: каналы передачи данных на пути от клиента к платформе, качество работы интернет-провайдера клиента, доступность облачного сервиса в данный момент времени. Также существует угроза того, что компания, предоставляющая облачные

услуги будет ликвидирована по тем или иным причинам, и клиент не сможет получить доступ к своим данным. Но, вне зависимости от этого, большинство экспертов придерживается того мнения, что преимущества данной технологии перевешивают ее недостатки.

В зависимости от нужд клиентов предоставляются несколько моделей реализации облачных технологий. Самой безопасной из них является модель частного облака, а наиболее уязвимой - модель публичного облака. Также облака делятся по моделям обслуживания. Каждая из них имеет свои преимущества и недостатки и выбирается пользователем исходя из преследуемых целей. Среди индивидуальных клиентов наибольшее распространение получила модель обслуживания SaaS. В настоящий момент времени все большее количество компаний предлагают свои приложения на основе данной модели. Но, в то же время, эта услуга по обработке информации является наименее безопасной.

В соответствии с поставленными задачами в данной работе были рассмотрены существующие модели угроз в облачных вычислениях и протестированы возможные меры по повышению безопасности пользовательских файлов. Методы аутентификации и разграничения доступа не были рассмотрены в силу того, что они не являются доступными рядовому пользователю.

В силу стремительного развития облачной инфраструктуры стоит ожидать появления в скором времени универсальных методов обеспечения безопасности данных. Но на сегодняшний день выделение наиболее оптимального метода защиты не является возможным, так как к каждому типу услуги должен быть применен индивидуальный подход в соответствии с преследуемыми целями заказчика облачных сервисов.

Список используемой литературы

1. Arif Mohamed. A history of cloud computing. http://www.computerweekly.com/feature/A-history-of-cloud-computing
2. Peter M. Mell, Timothy Grance The NIST Definition of Cloud Computing https://www.nist.gov/node/568586
3. SoCC 10: Proceedings of the 1st ACM symposium on Cloud computing / Hellerstein, Joseph M. - N. Y.: ACM, 2010. - ISBN 978-1-4503-0036-0.
4. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — 379 p
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ
6. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" / СЗ РФ. 2006. N 31 (ч. 1). Ст. 3451.
7. Риз Дж. Облачные вычисления. Пер. с англ. — СПб.: БХВ-Петербург, 2011.
8. Гребнев Е. Облачные сервисы. Взгляд из России – М.: CNews, 2011. – 282
9. Глазунов С. Бизнес в облаках. Чем полезны облачные технологии для предпринимателя. https://kontur.ru/articles/225.
10. Иванников В.П. Отчет ИСПРАН «Облачные вычисления в образовании, науке и госсекторе» / ИНИОН РАН. М., 2013
11. Бузов Г.А., Калинин СВ., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие.- М.- Горячая линия-Телеком.- 2005.-416 с.
12. Лебедь С. В., Межсетевое экранирование: Теория и практика защиты внешнего периметра, Издательство Московского технического университета им. Баумана, 2002 г, 304 с.
13. Панасенко С.П. Алгоритмы шифрования. Специальный справочник BHV-Санкт-Петербург, 2009. – 576с.
14. Туманов Ю.М. Защита сред облачных вычислений путем верификации программного обеспечения на наличие деструктивных свойств // Автореф. канд. дисс., М.: Изд-во НИЯУ «МИФИ», 2012. 20 с.
15. Грейс Уокер, «Основы облачных вычислений», Справочник IBM, 2013г.
16. Иванников В.П. Отчет ИСПРАН «Облачные вычисления в образовании, науке и госсекторе» / ИНИОН РАН. М., 2013
17. Савченко А.П. Корпоративная база знаний как ядро системы управления знаниями организации // Научное, экспертно-аналитическое и

информационное обеспечение национального стратегического проектирования, инновационного и технологического развития России ИНИОН РАН, Москва, 2009. С. 297-300
18. Разумников С.В. Интегральная модель оценки эффективности и рисков облачных ИТ-сервисов для внедрения на предприятие // Фундаментальные исследования. – 2015. – № 2-24. – С. 5362-5366;
19. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных / Мир Internet. – М.: №2, 2001;
20. Бердник А. В. Сравнительный анализ решений по безопасности SaaS сервиса от компании IBM и КРОК // Безопасность информационного пространства: сборник статей. Тюмень, 2012. С. 245-253.
21. Вихорев С., Кобцев Р. Как определить источники угроз.//Открытые системы. – 2002. - №07-08.С.43.
22. Краковский Ю.М.: Информационная безопасность и защита информации. - М. ; Ростов н/Д: МарТ, 2008
23. 8 шагов к безопасным облачным системам // Журнал «Information Security/Информационная безопасность» № 1, 2013. - С. 28-29
24. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001, — 368 с.
25. Панасенко С.П. Алгоритмы шифрования. Специальный справочник BHV-Санкт-Петербург, 2009. – 576с.
26. Рябко Б. Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004.
27. «Гигиеническими требованиями к персональным электронно-вычислительным машинам и организации работы» (СанПиН 2.2.2 / 2.4.1340-03);
28. «Типовой инструкцией по охране труда при работе на персональном компьютере» (ТОИ Р-45-084-01).
29. Безопасность жизнедеятельности. Безопасность технологических процессов и производств (Охрана труда): Учебн. пособие для вузов / П.П. Кукин, Е.А. Подгорных и др. – М.: Высш.шк., 1999. – 318 с.: ил.
30. Бурлак Г.Н. Безопасность работы на компьютере. Организация труда на предприятиях информационного обслуживания. – Учеб. пособие. – М.: Финансы и статистика, 1998. – 144 с.

Приложение 1

Сравнение типов подключения

Подключение	Требования на стороне сервис-провайдера	Подключение клиента	Плюсы	Минусы
RDP-клиент	Наличие выделенного сервера терминалов (Terminal Server)	Запуск клиента RDP	Мультиплатформность, гибкая система настройки	Слабое шифрование при использовании настроек по умолчанию, необходимость использовать дополнительные методы защиты
RemoteApp	Наличие сконфигурированного RD Session Host Server с размещенным на нем списком соответствующих программ (RemoteApp Programs list)	Запуск иконки приложения с рабочего стола или из меню Start для инициирования подключения к приложению по RDP (из списка RemoteApp Programs list).	Обеспечение доступности приложения в условиях неизкой скорости интернета, позволяет совмещать работу на локальной машине и использования приложения в облаке	Дает доступ только к одному приложению
Веб-доступ	Наличие выделенного сервера терминалов (Terminal Server)	Использование URL для доступа к ресурсу посредством веб-браузера.	Легкость использования	Нет защищенной линии передачи, требуется проходить аутентификацию

Remote access VPN	Наличие сконфигурированного VPN-сервера	Запуск ярлыка для подключения к VPN-серверу.	Не надо устанавливать дополнительные приложения	Наличие VPN-сервера на стороне провайдера, необходимо проходить аутентификацию
VPN site-to-site	Наличие двух сконфигурированных VPN-серверов.	При обращении к ресурсам VPN-подключение организуется автоматически и на уровне серверов	Отсутствие необходимости создания и запуска ярлыка VPN-подключения, прозрачно для конечного пользователя	Необходим VPN-сервер в компании и VPN-сервер в облаке
DirectAccess	Наличие одного или более серверов DirectAccess в составе домена, Наличие центра сертификации (PKI), Windows-инфраструктура	При наличии доступа к сети Интернет происходит автоматическое построение надежного туннеля между клиентом и сервером	Доступ к ресурсам компании прозрачен для пользователя, Физическое местоположение клиента не имеет значения	Ограниченный список клиентских ОС, с которых возможно подключение: Windows 7 Enterprise или Windows 7 Ultimate, Компьютер клиента должен входить в состав домена.
VDI	Развернутая инфраструктура виртуальных рабочих столов VDI (решения от VMware, Citrix, Microsoft)	Пользователь получает свой собственный виртуальный ПК	Можно подключаться с помощью тонкого клиента, настольного ПК, ноутбука, планшета, мобильного телефона	При сбое в приложения в терминальном режиме вместе с пользователем, запустившим такое приложение, перезагрузятся и остальные пользователи, работающие на этом же сервере

Приложение 2