Правительство Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего профессионального образования

«Национальный исследовательский университет   
«Высшая школа экономики»

**Факультет бизнес-информатики**

###### **Кафедра информационной безопасности**

###### **ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

На тему**:**

**«**Обеспечение безопасности информации клиентов в облачных сетях»

Студент группы № 475  
Прохоров Вадим Станиславович

Научный руководитель  
Елин Владимир Михайлович

Москва 2013

Оглавление

[Введение 4](#_Toc357777246)

[Глава 1. Защита информации в облачных технологиях 7](#_Toc357777247)

[1.1. Общие методы обеспечения информационной безопасности 7](#_Toc357777248)

[1.1.1. Информационная безопасность и возможные угрозы 7](#_Toc357777249)

[1.1.1.1. Понятие информационной безопасности 7](#_Toc357777250)

[1.1.1.2. Угрозы информационной безопасности 9](#_Toc357777251)

[1.1.2. Общие методы применяемые для безопасности информации 12](#_Toc357777252)

[1.3. Характеристика услуг в облаке 13](#_Toc357777253)

[1.3.1. Понятие облачных вычислений 13](#_Toc357777254)

[1.3.2. Виды «облаков» 14](#_Toc357777255)

[1.3.3. Плюсы и минусы использования облачных технологий 17](#_Toc357777256)

[1.4. Проблематика защиты 21](#_Toc357777257)

[1.4.1 Аппаратные компоненты центра обработки данных 24](#_Toc357777258)

[1.4.2. Телекоммуникационная составляющая доступа к ресурсам центра обработки данных 24](#_Toc357777259)

[1.4.3. Пользователи и их программно-аппаратное обеспечение 25](#_Toc357777260)

[1.4.4 «Средний» (middleware) слой центра обработки данных 26](#_Toc357777261)

[1.4.5 Прикладные сервисы 26](#_Toc357777262)

[1.4.6 Системы хранения данных 27](#_Toc357777263)

[Глава 2. Принципы защиты данных действующие в странах-членах Европейского союза 28](#_Toc357777264)

[2.1 Риски по защите информационной безопасности в облачных вычислениях 28](#_Toc357777265)

[2.1.1. Отсутствие контроля 28](#_Toc357777266)

[2.1.2. Отсутствие прозрачности 30](#_Toc357777267)

[2.2. Правовая основа 31](#_Toc357777268)

[2.2.1. Структура защиты данных 31](#_Toc357777269)

[2.2.2. Применяемы правовые нормы 31](#_Toc357777270)

[2.2.3. Обязанности и ответственности сторон 33](#_Toc357777271)

[2.2.3.1 Клиент и провайдер в облаке 33](#_Toc357777272)

[2.2.3.2. Субподрядчики 36](#_Toc357777273)

[2.2.4. Требования по защите данных в отношениях сторон 38](#_Toc357777274)

[2.2.4.1. Соблюдение основных принципов 38](#_Toc357777275)

[2.2.4.2. Договорные гарантии отношений «контроллер» - «процессор» 42](#_Toc357777276)

[2.2.4.3. Технические и организационные меры по защите и безопасности данных 46](#_Toc357777277)

[2.2.5. Международные передачи 52](#_Toc357777278)

[2.2.5.1. SafeHarbor и отвечающие требованиям страны 53](#_Toc357777279)

[2.2.5.2. Исключения 55](#_Toc357777280)

[2.2.5.3. Стандартные условия договора 55](#_Toc357777281)

[2.2.5.4. Обязательные корпоративные правила на пути к глобальному подходу 56](#_Toc357777282)

[Заключение 58](#_Toc357777283)

[Библиографический список 62](#_Toc357777284)

**Введение**

Мы живем во время стремительного роста информационных технологий, идет колоссальное развитие программного обеспечения. Раньше разработанные программистами приложения распространялись на физических носителях, после чего их необходимо было устанавливать на компьютер. Для корректной работы программ персональный компьютер должен был отвечать минимальным системным требованиям, выставленными разработчиками программного обеспечения. Развивался Интернет, модернизировалось и серверное оборудование. И в какой-то момент оказалось, что можно объединить вычислительные мощности для поддержки программных сервисов – например, текстовые и табличные процессоры. Это и стало отправной точкой в развитии «облачных» вычислений.

Актуальность данной работы определяется тем обстоятельством, что на данный момент практически каждый пользователей компьютера сталкивался в своей работе с облачными вычислениями.

Повсеместное использование ЭВМ и, на их основе, всевозможных организационно-технических («человек-машина») систем, таких как «облачные» вычисления, влечет за собой возникновение проблем информационной безопасности.

В законе РФ «Об информации, информатизации и защите информации» подчеркивается, что «информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства».

Вопросы безопасности информации занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация.

Учитывая изложенное, целью настоящей работы является изучить специфику защиты информации клиентов облачных сетей, а именно исследовать положения по обеспечению безопасности информации в странах-членах ЕС.

Исходя из поставленной цели определен следующий круг задач:

1. Изучить общие понятия информационной безопасности и облачных вычислений;
2. Проанализировать общие методы обеспечения информационной безопасности;
3. Исследовать проблематику защиты информации в облачных технологиях.

Объектом исследования в настоящей работе являются

Предметом исследования в настоящей работе является изучение принципов защиты информации в облачных сервисах действующих в Европейском экономическом пространстве.

Структура настоящей работы состоит из:

1. Первая глава включает в себя

* рассмотрение общих понятий информационной и компьютерной безопасности, разбор видов возникающих угроз, а также разбор характеристик общих методов по защите от этих угроз.
* разбор структуры работы облачных вычислений, начиная с рассмотрения видов облаков и заканчивая проблематикой защиты данных на каждом этапе работы облачного сервиса.

1. Вовторой главе приведен подробный анализ ситуации по обеспечению безопасности информации в странах-членах Европейского союза: разобраны риски и правовая основа участников информационных отношений.

# Глава 1. Защита информации в облачных технологиях

## 1.1. Общие методы обеспечения информационной безопасности

### 1.1.1. Информационная безопасность и возможные угрозы

#### 1.1.1.1. Понятие информационной безопасности

Под термином «информационная безопасность» можно понимать несколько различных значений, в условии от контекста, в котором данное словосочетание употребляется. Если рассмотреть использование термина в Доктрине информационной безопасности Российской Федерации, там определение дано в большом спектре. В нем учитывается совокупность личностных, общественных и государственных интересов в национальных масштабах[[1]](#footnote-2).

Понятие «информационной безопасности» в Законе РФ «Об информации, информационных технологиях и о защите информации» понимают примерно тоже самое – некое состояние информационной среды, при которой соблюдаются интересы граждан, организаций и государства[[2]](#footnote-3).

В ходе данной работы будут рассмотрены этапы хранения, обработки и передачи информации независимо от вида ее кодирования, от вида объекта или, непосредственно, от самой смысловой нагрузки. Из-за этого круг использования термина «информационная безопасность» значительно снижается.

В нашем случае, под «информационной безопасностью» мы будем понимать степень защиты информации и обеспечивающие ее существование инфраструктуры от нежелательного (случайного и специального) воздействия, которое в дальнейшем способно нанести неприемлемый ущерб участникам информационных отношений.

В защиту информации входит набор мероприятий по защите информационной безопасности.

Поэтому, для выявления проблем информационной безопасности, сначала необходимо определить участников данных отношений и их интересов, касательных использования информационных систем. Угрозы информационной безопасности это неотъемлемая часть, возникающая всегда при использовании информационных технологий.

Поэтому приведем два важных заключения:

1. В соответствии с различием категорий субъектов в информационных отношениях, проблемы, возникающие в процессе, существенно различаются. Эту ситуацию можно рассмотреть на контрастном примере в случае государственной организации и среднего учебного заведения. Для первого субъекта лучше уничтожить все данные, чем допустить вероятность их утечки. Во втором наоборот - главное чтобы все работало, никаких секретов не хранят.
2. В задачах информационной безопасности стоит не только защита, в целях предотвращения от нежелательного доступа к информации. Участники информационных отношений могут понести ущерб еще и от проблем, связанных с функционированием системы, которая ведет к сбоям в работе. Тем более, как упоминалось выше, защита от несанкционированного доступа к информации для таких организаций, как школьные заведения, стоит не на первом месте.

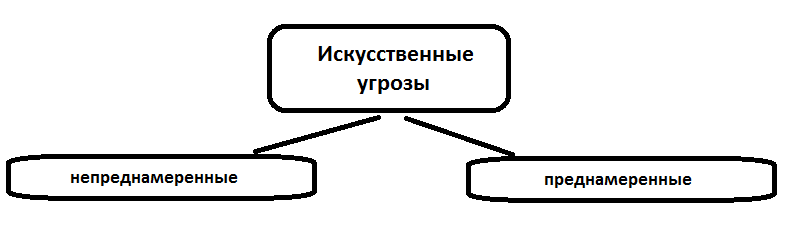
Возвращаясь к определениям, стоит сказать, что под термином «компьютерная безопасность» подразумевается не только процесс обработки хранения, происходящие на компьютере. Так как компьютер является лишь частью в цепочки обращения информации, лишь малая часть, которая составляет информационные системы. Поэтому информационная безопасность напрямую зависит от поддерживающей инфраструктуры, к элементам которой относятся системы электроснабжения, теплоснабжения, охлаждающие системы, обслуживающий персонал[[3]](#footnote-4).

Невозможно предугадать и предотвратить все угрозы безопасности информации. Недаром в нашей трактовке термина «информационной безопасности» присутствует словосочетание «неприемлемый ущерб». Меры по обеспечению безопасности могут оказаться огромными, с экономической точки зрения. Поэтому, любые возможные риски нужно адекватно оценивать и сопоставлять с затратами по их предотвращению. Но есть ряд угроз, таких как, возможный ущерб состоянию здоровью человека или окружающей среды, которые относятся к категории недопустимых угроз. Поэтому в их отношении необходимо применять все меры по предотвращению.

#### 1.1.1.2. Угрозы информационной безопасности

Существует два основных типа угроз информационной безопасности[[4]](#footnote-5):

* Искусственные,
* Естественные.



Непреднамеренными угрозами считаются действия, совершенные людьми из-за отсутствия должного внимания, необходимой осторожности, достаточных знаний.

К примерам непреднамеренному типу угроз можно отнести излишнею установку программного обеспечения, которое не является необходимым для работы. В дальнейшем эти избыточные продукты могут стать причиной сбоя в работе. Так же можно привести в пример такую человеческую особенность, как любопытство. Совершенные действия по незнанию не являются злым умыслом, но могут стать причиной ущерба. Такой тип угроз сложно предусмотреть и проконтролировать[[5]](#footnote-6).

Преднамеренными угрозами считаются угрозы, преднамеренно направленные на физическое разрушение с последующим выходом системы из строя.

К примерам такого типа угроз можно отнести атаки на информационную систему, внутреннего и внешнего характера. Зачастую внутренней защите информационной системы уделяют куда меньше внимания, чем внешней защиты. Истории известны случаи многомиллионных потерь в крупных компаниях из-за внутреннего взлома системы и кражи данных.

Также искусственные угрозы можно разбить по категориям:

1. Действия пользователей, которые авторизовались в системе:

* хищение или уничтожение данных,
* повреждение данных по неосторожности.

1. Воздействие «электронного» характера.

Под этим понимаются действия хакеров, с целенаправленным взломом системы для извлечения выгоды, либо просто из любопытства. Примером является несанкционированный доступ к данным, целью которого является проникновение в корпоративную сеть предприятия извне. При получении доступа к данным, хакеры используют ее для нанесения вреда. Используя сетевую инфраструктуру, хакеры могут производить атаки не только на узлы предприятия, но и на узлы третьих фирм, конфиденциальная информация о которых храниться на атакованном предприятии.

1. Компьютерные вирусы.

Для современного ведения бизнеса компьютерные вирусы являются серьезной угрозой. На данный момент практически любая компания имеет свою информационную систему и активно ее использует в работе. Заражение корпоративной сети компьютерными вирусами может привести к отказу работы всех информационных сервисов, перебоям в работе, хищению данных или их уничтожению. Проникновение вирусных программ в сеть предприятия может дать злоумышленником полный или частичный контроль над всеми операциями компании.

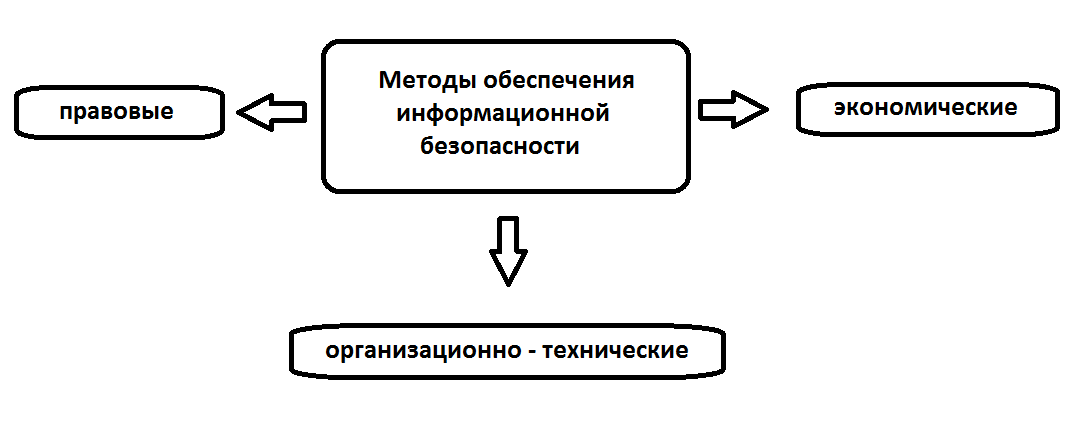
1. Спам.

Темпы роста воздействия угрозы спама с каждым годом все больше. Спам нагружает избыточной и ненужной информацией, которая может оказаться вредоносной. Большим каналом для распространения спама является электронная почта.

С естественными угрозами ситуация куда-более очевидна. К данному типу угроз относится кража физического оборудования с информацией, к примеру, компьютера или различных носителей. Так же к ним относятся все виды стихийных бедствий: цунами, ураганы, удары молний, пожары.

Угроза пожара случается наиболее часто. В данной ситуации, меры по обеспечению пожарной безопасности относятся не только к обеспечению безопасности жизни людей, но и безопасности информации.

### 1.1.2. Общие методы применяемые для безопасности информации



**Правовые методы**

Правовые методы по обесп6ечению безопасности включают в себя разработку нормативно-правовых актов, регламентирующих информационные отношения между участниками, и нормативно-методических документов, отражающих вопросы по обеспечению информационной безопасности[[6]](#footnote-7).

Особенно важными в этой деятельности являются следующие действия:

* своевременное внесение изменений и дополнений, касающихся регулированию отношений в сфере безопасности информации, в законодательство государства;
* устранение противоречий, связанных с международными соглашениями;
* установление ответственности за правонарушения;
* разграничение полномочий в области обеспечения информационной безопасности;
* разработка и принятие нормативных правовых актов.

**Организационно-технические**

К такие методам относятся:

* создание и модернизация системы по обеспечению информационной безопасности;
* усиление исполнительной власти касательно правоприменительной деятельности;
* разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств;
* выявление технических устройств и программ, представляющих опасность для безопасности информации;
* сертификация средств защиты информации;
* контроль за действиями персонала в защищенных информационных системах;
* формирование системы мониторинга показателей и характеристик информационной безопасности.

**Экономические**

Экономические методы по предоставлению безопасности в себя включают:

* разработка планов по обеспечению информационной безопасности;
* совершенствование системы финансирования работ, связанных с организацией правовых и организационно-технических методов.

## 1.3.Характеристика услуг в облаке

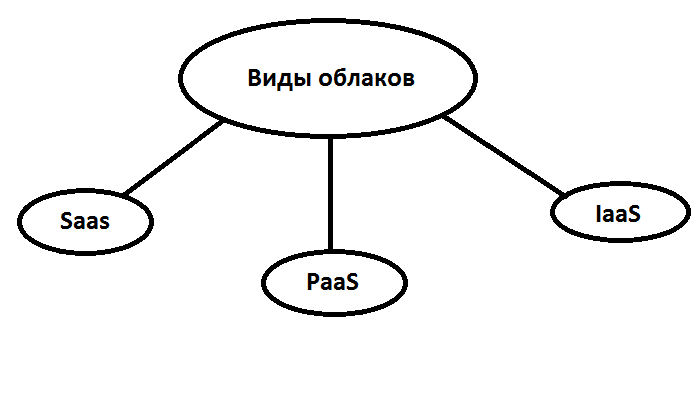
### 1.3.1. Понятие облачных вычислений

Cloud computing, что в переводе с английского означает – облачные вычисления. Cloud computing — технология предоставления пользователю по средствам сети Интернет возможности использования удаленных ресурсов и мощностей. Данная технологи происходит по принципу распределенной обработки данных. Ее суть заключается в обеспечении пользователя удаленным доступом к предоставляемым в облаке услугам. Потребность в экономии средств за счет эффективных мер по оказанию услуг в сфере хостинга повлияла на развитие технологии[[7]](#footnote-8).

Под термином «облачные вычисления» сегодня понимают набор различных сервисов, доступ к которым осуществляется через сеть Интернет. Облачные технологии представляют собой мощное решение, связанное с решением ресурсоемких задач. Популярность использования все время растет. Все пользователи персональных компьютеров либо обращались к услугам облачных сервисов, либо уже активно их используют.

## 1.3.2. Виды «облаков»

Понятие облачных вычислений имеет широкий спектр применения. Поэтому имеет смысл его логического разделения на несколько групп.



1. *SaaS: программное обеспечение как услуга*

SaaS - услуга облачных приложений или "Software as a Service ", вероятно, наиболее популярная простая в использовании форма облачных вычислений. SaaS использует сеть Интернет для доставки приложений, которые управляются сторонними поставщиками и чей интерфейс доступен клиентской стороне. Большинство SaaS приложений можно запускать непосредственно из веб-браузера, без необходимости загрузки или предварительной установки. SaaS избавляет от необходимости устанавливать и запускать приложения на персональных компьютерах. С использованием SaaS, упрощается задача предприятий по рационализированию технического обслуживания и поддержки, потому что в услуги поставщика входит обслуживание: приложений, времени выполнения, данных, промежуточного ПО, операционных систем, виртуализации серверов, хранилищ и сеть. Gmail является одним известным примером почтового оператора SaaS.

1. *PaaS: платформа как услуга*

PaaS - самый сложный из трех видов - облачная платформа услуг или "Platformas as Service" распределяет вычислительным ресурсы через платформу. Разработчики получают с PaaS возможность, где они могут создать для разработки или настройки приложений. PaaS делает разработку, тестирование и развертывание приложений быстрее, проще и экономично эффективным, избавляя пользователя от необходимости покупать нижележащие слои аппаратного и программного обеспечения. Одно различие между SaaS и PaaS связано с тем, что некоторые аспекты в PaaS должны уже управляться пользователями, а не поставщиками: С PaaS, поставщики до сих пор контролируют: время выполнения, промежуточное ПО, операционную систему, виртуализацию серверов, хранилище и сети, но пользователям управлять приложениями и данными.

PaaS предоставляет вычислительные инфраструктуры, оборудование и платформы, которые установлены на верхней части аппаратного обеспечения. Подобно тому, как вы можете создавать макросы в Excel, PaaS позволяет создавать приложения, используя программные компоненты, которые управляются с помощью стороннего поставщика. PaaS является хорошо масштабируемым, и пользователям не придется беспокоиться об обновлении платформы или их сайт выйдет из строя во время технического обслуживания. Пользователи, которые получают наибольшую отдачу от PaaS, составляют компанию, которая хочет повысить эффективность и интерактивность большого штата. Для нужд крупных компаний и независимых поставщиков программного обеспечения Apprenda является одним поставщиком для личного PaaS разработки и развертывания бизнес-приложений.

1. *IaaS: инфраструктура как услуга*

IaaS - облачная инфраструктура услуг, известная как "Infrastructure as a Service " поставляет компьютеру инфраструктуру (например, платформу виртуализации среды), хранилище и сеть. Вместо того, чтобы приобретать программное обеспечение, сервера или сетевое оборудование, пользователь может купить все это как полностью внешний сервис, счет за который обычно зависимости от количества потребляемых ресурсов. Другими словами, третья сторона за арендную плату позволяет установить виртуальный сервер на их ИТ-инфраструктуре. По сравнению с SaaS и PaaS, IaaS пользователи несут большую ответственность за управление: приложениями, данными, временем выполнения, промежуточным ПО и операционными системами. Поставщики услуги по-прежнему контролируют виртуализацию, сервера, жесткие диски, хранилища и сеть. Пользователи IaaS получают возможность полного доступа к готовой информационной инфраструктуре, внутри которой они могут установить необходимые платформы. Пользователи несут ответственность за обновление, если новые версии платформ вышли.

Еще необходимо назвать одно ключевое разделение облаков: публичные и частные. Услуги, предоставляемые публичными облаками, могут быть доступны любому пользователю. Ярким примером публичного облака является Amazon Web Services. Главная разница между публичными и частными облаками в том, что к последним осуществляется закрытый доступ только для ограниченного числа пользователей.

### 1.3.3. Плюсы и минусы использования облачных технологий

*Достоинства:*

•Сравнительно дешевые компьютеры для пользователей. Проподает необходимость приобретать компьютеры высокой мощности с большим объемом памяти и дисков, так как вся информация и все программы хранятся на серверах в «облаке» и запускаются удаленно. С больших стационарных персональных компьютеров и обычных ноутбуков пользователи могут перейти на компактные нетбуки[[8]](#footnote-9).

•Выросла производительность компьютеров для пользователей. Из-за удаленного запуска большей части файлов и программ компьютеры пользователей, не обремененные этой работой и с меньшим числом приложений, функционируют быстрее. Как пример можно рассмотреть работу Panda Cloud Antivirus – программа антивирус, доступная как вебсервис. Panda Cloud Antivirus предоставляет возможность сканировать данные на вирусы удаленно на мощных серверах. Запуск этой же программы непосредственно на самом компьютере пользователя с помощью его собственных ресурсов увеличивало бы нагрузку в 2 раза.

•Повышается эффективность использования IT инфраструктуры и идет снижение затрат. Если взять среднюю оценку загрузки сервера для компании, то она составит около 13%. Иногда для компании появляется необходимость использовать дополнительные мощностные ресурсы, но большинство времени вычислительные ресурсы ничем не заняты. Идет простой – деньги на ветер. Если же использовать вычислительные ресурсы на удаленных серверах в «облаке» по мере необходимости, то затраты компании по этой части могут сократиться вдвое. С учетом непостоянной экономической обстановки гибкость производства возрастает. Компании, которые не доверяют сохранность своих данных сторонним организациям, имеют возможность построить свое собственное облако и получать все преимущества от виртуализации инфраструктуры.

•Снижение затрат на обслуживание и приобретаемое ПО. С использованием технологии CloudCimputing собственных серверов у компаний становится меньше, поэтому обслуживать их становится легче. С избавлением от большого количества физических серверов проблемы с приобретением программного обеспечения также уменьшаются. Так как сервисы и приложения находятся в «облаке», нет необходимости приобретать ПО для каждого пользователя. Компания приобретает нужные программы в «облаке». Стоимость сервисов, предлагаемых с доступом через Инернет, на порядок ниже аналогов, которые существуют для персональных компьютеров. Более того, есть возможность повременной аренды использования программ, а затраты на поддержку ПО в рабочем состоянии и его обновление равны нулю.

•Рост вычислительной мощности. В сравнении с персональным компьютером, вычислительные ресурсы облака предоставляют огромные возможности. Вычислительная мощность облака определяется количеством его серверов. Иначе говоря, пользователям предоставляется удаленный доступ к суперкомпьютеру, который дает возможность решать более сложные и объемные задачи, непосильные обычному ПК.

•Неограниченный объем для хранения данных. Объем предоставляемого места в облаке для хранения данных может гибко и автоматически подстраиваться, в зависимости от пожеланий пользователя. Если для пользователя персональным компьютером обычна ситуация недостатка места для данных, то для пользователя облачных вычислений это практически невозможно.

•Совместимость с операционными системами. Для облачных технологий неважно, какая операционная система стоит у пользователя. Клиент с системой Microsoft Windows может без проблем обмениваться данными через облако с пользователями системы Unix. Что касается доступа к сервисам облачных вычислений, то они предоставляются с помощью стандартных для каждой операционной системы браузеров.

•Совместимость форматов документов. На персональном компьюторе файл, сделанный в программе MicrosotWord 2007, не сможет открытся более ранней версией MicrosoftWord 2003. В облачных вычислениях отсутствует понятие несовместимости форматов документов, созданных в разных версиях одной облачной программы.

•Легкость совместной работы для группы пользователей. В системе облачных вычислений появляется удобная возможность одновременной работы нескольких участников. Нет нужды заниматься переносом документов с компьютера на компьютер. Редактирование документов отражается мгновенно, причем пользователю всегда доступна последняя версия обновленного документа.

•Повсеместный доступ к файлам пользователя является большим преимуществом использования облачных вычислений. Если данные хранятся в облаке, они всегда доступны для их обладателя при наличии доступа в сеть Интернет. Также перед пользователем открывается широкий выбор различных устройст, с которых он может осуществить этот доступ. Клиент облака может воспользоваться персональным компьютером, нетбуком, ноутбуком, планшетным компьютером, смартфоном.

•Уменьшение использования ресурсов природы. С технологией облачных вычислений экономия идет не только на электроэнергии, вычислительных мощностях и физическом пространстве, но и и на ресурсах природы. Центры обработки данных можно располагать уже заведома в прохладном климате. Оборудование для доступа к данным теперь более компактное, требует для изготовления меньше материалов.

•Устойчивость данных к потере. Данные, хранящиеся на облаке, распределяют свои копии по нескольким серверам. Вероятность потери данных в облаке куда меньше вероятности их потери при хранении на обычных физических носителях информации.

*Недостатки:*

•Постоянная необходимость соединения с сетью Интернет. Для технологии облачных вычислений всегда необходимо соединение с сетью Интернет. Существует, конечно, ряд приложений, которые загружаются на компьютер и позволяют дальнейшую работу не смотря на соединение. В остальных случаях все просто: нет соединения – нет работы. По мнению многих, это самый большой недостаток облачных вычислений. Но если учесть развитие информационных технологий в наше время, то можно с уверенностью сказать, что доступ в сеть Интернет есть практически везде. Поэтому в скором времени такая проблема и вовсе исчезнет.

•Плохо работает с медленным соединением. Большинство облачных сервисов требуют для нормальной работы быстрое Интернет-соединение. Но как говорилось выше, информационные технологии не стоят на месте, поэтому сейчас нет проблем с пропускной способностью соединений сети Интернет.

•Программы могут работать медленно и с неполными функциональными возможностями. Некоторые из программ, предоставляемые облачными услугами, работают на локальном компьютере быстрее. Это может быть связано как с невысокой пропускной способностью соединения сети Интернет, так и загруженностью удаленных серверов. Также, программы, представленные в облаке, имеют ограниченный функционал, в отличии от их версий для локального компьютера.

•Существует угроза безопасности данных. Безусловно, если вы передаете ваши данные в облако, то сразу возникает возможность угрозы безопасности информации. Но тут все дело заключается в доверии к провайдеру. Если поставщик облачной технологии надежно шифрует передвижение информации, создает резервные копии и уже имеет большой опыт на рынке в данной сфере, то нарушение системы безопасности может никогда не случится.

Факт, что потеря данных в облаке является безвозвратной. Но довести до такого состояния куда более сложно, чем потерять их на локальном компьютере.

Не смотря на преобладающие множество достоинств над недостатками, в каждой ситуации все происходит по-разному. Каждый сам оценивает все критерии и принимает выбор: использовать облачные вычисления или нет.

## 1.4. Проблематика защиты

В течение последнего времени постоянно поднимается вопрос о перспективе развитие облачных вычислений, рассматриваются планы развития данной технологии. Это связано с колоссальным приростом бизнеса, который с каждым годом увеличивает свой темп. Основная суть технологии облака заключается в предоставлении различных информационных платформ, приложений для пользователя через сеть Интернет. Принцип идеи заключается в освобождении ресурсов персонального компьютера пользователя, и перенос этой нагрузки на удаленные вычислительные мощности. ЦОДы, или центры обработки данных – решение к данному подходу. Гигантские вычислительные мощности, находящиеся удаленно, предоставляют возможность практически неограниченного места для хранения данных, огромную вычислительную производительность и мгновенный доступ к данным любому пользователю-клиенту по средствам интернет соединения. Аналогично имеется возможность для компаний создавать собственные облака, где сотрудники пользуются всеми привилегиями данной технологии, рядовому сотруднику достаточно лишь иметь доступ к корпоративной сети. В таких условиях пользовательская сторона процесса является наиболее важной[[9]](#footnote-10). При данной ситуации вопрос об информационной безопасности отодвигается на второй план. Идет интенсивная рекламная компания, представляющая облачные вычисления как нечто принципиально новое, поэтому решенные проблемы информационной безопасности откладываются на позднее время, ставя под угрозу не только данные пользователей, но и устойчивость всей структуры в целом. Данная ситуация напоминает процесс развития электронного «банкинга» в течение последних десяти лет, где вопросы по безопасности информации стали интенсивно решаться вследствие больших потерь, достигающих десять, а то и пятнадцать процентов от прибыли.

Аналогию процессов облачных вычислений можно увидеть в больших вычислительных системах 80-х годов прошлого века, где основным различием была лишь широта возможностей по высокоскоростному доступу пользователей к ресурсам вычислительных центров. И такой доступ был возможен только на территории отдельных организаций, которые использовали эти центры для вычислений. Но уже в 90-х годах, когда скорость вычислений превзошла скорость обработки и подготовки информации в периферийных устройствах, была реализована возможность параллельного решения задач на одном вычислительном устройстве[[10]](#footnote-11).

Как процесс развития «облачных» вычислений зародился несколько десятков лет назад, так и подходы к информационной безопасности. Основные принципы по обеспечению безопасности информации в компьютерных системах, которые удалось разработать за последние 20 лет, можно использовать и в облачных вычислениях. В статье Баранова А.П. «Можно ли защитить в облаке конфиденциальную информацию?» рассмотрена эта возможность применения, а так же раскрыты нерешенные проблемы, которые сдерживают развитие в области безопасности информации для вычислений в «облаке».

Для анализа взята организация «облачных» вычислений на основе центра обработки данных, реализующего принцип виртуализации вычислений.

Автор разбивает систему вычислений в «облаке» на шесть основных частей[[11]](#footnote-12):

1. Аппаратные компоненты центра обработки данных.

2. Телекоммуникационная составляющая доступа к ресурсам центра обработки данных.

3. Пользователи и их программно-аппаратное обеспечение.

4. «Средний» (middleware) слой центра обработки данных.

5. Прикладные сервисы.

6. Системы хранения данных (СУБД).

В своей статье автор рассматривает проблему обеспечений безопасности информации в каждой из приведенных выше частей, подразделяя применение каждой из них по двум возможным направлениям: корпоративные и публичные системы.

### 1.4.1 Аппаратные компоненты центра обработки данных

Основные принципы выбора аппаратных средств, с последующей их аттестацией, для обработки конфиденциальной информации в корпоративных сетях хорошо и давно известны. Выбор основывается на гарантии качества, отличающейся надежностью и устойчивостью в работе. Гарантию предоставляют производители аппаратных компонентов. Также необходимо отметить ряд необходимых организационных и технических мер по предотвращению несанкционированного доступа к аппаратной части центров обработки данных. Бывают ситуации, когда хакер пытается нарушить режим информационной безопасности. Поэтому постоянно ведется контроль на определение побочных сигналов или электромагнитных воздействий. В таких случаях определенными методами проводится исследование сигналов и защита от внешнего воздействия. Подобные действия при аналогичной ситуации проводятся для систем облачных вычислений с публичным доступом[[12]](#footnote-13).

### 1.4.2. Телекоммуникационная составляющая доступа к ресурсам центра обработки данных

Принцип работы завязан на двух основных методах: шифрование IP-пакетов при помощи аппаратных и программных средств, либо просто на открытом трафике. Практически всегда в корпоративных сетях компаний необходимо сохранять конфиденциальность обрабатываемых персональных данных для того, чтобы была возможность доступа через IP-сети. Поэтому, как правило, телекоммуникационная составляющая основывается на шифровании IP-пакетов. Все кодирование пакетов занимает у системы значительную часть ресурсов и может растягиваться во времени. Снижение уровня шифрования приводит к увеличению открытого трафика, что способствует падению уровня защиты конфиденциальной информации. В некоторых сферах деятельности человека данная ситуация недопустима. Поэтому, актуальной задачей является повышение скорости IP-шифрования.

### 1.4.3. Пользователи и их программно-аппаратное обеспечение

В настоящее время не составляет никаких проблем, с точки зрения программных и аппаратных средств, по шифрованию IP-потока по SSL протоколу на пользовательском рабочем месте. Скорость обработки без проблем может достигать 1Мбит/с. На данный момент имеется достаточно сертифицированных фирм, предоставляющих соответствующие услуги. Гораздо сложнее обеспечить информационную безопасность по защите ключей пользователя, его операционной системы и личной информации в корпоративном облаке. На персональные компьютеры сотрудника устанавливаются электронные замки. Данную блокировку может контролировать не только пользователь заблокированного рабочего места, но и служба информационной безопасности компании. Но это все касается частных систем, все более сложно складывается для публичных облаков. Получить легальные права доступа к системе может любой пользователь. Здесь нарушителям, с помощью специальных программных и технических средств, устанавливаемых непосредственно на рабочем месте, гораздо легче преодолеть защиту системы безопасности. Невозможно проконтролировать всех пользователей сети Интернет на состав рабочего места и предугадать их намерения. Поэтому в ЦОД публичных сетей должны быть максимально эффективные средства защиты, которые постоянно находились бы под жестким контролем.

### 1.4.4 «Средний» (middleware) слой центра обработки данных

Центр обработки данных по своей структуре – это виртуальная машина. Соответственно, в роли гипервизора и набора различных гостевых операционных систем в данной машине можно считать «средний» слой ЦОД. К виртуальным машинам также относится и управляющая система. Известный факт, что при создании и последующей эксплуатации виртуальных машин, гипервизор играет ключевую роль, как основной элемент системы информационной безопасности. Являясь, в свою очередь, операционной системой, гипервизор работает с аппаратным программным обеспечением, имеет возможность распределять функции от базовой системы гостевым. Поэтому, гипервизор можно смело сравнивать со стандартной операционной системой. Таким образом, для обеспечения нормального функционирования системы в режиме информационной безопасности, необходимо применять к гипервизору требования, которые используются для классических операционных систем.

### 1.4.5 Прикладные сервисы

Прикладные сервисы можно сравнивать с прикладным программным обеспечением операционных систем, которые проходят сертифицированную аттестацию в сфере информационной безопасности. Период проверки всех требований к программному обеспечению во время этапов сертификации операционных систем занимал не более квартала. Для крупных сервисов облачных вычислений, таких как MicrosoftWord или Explorer, потратили около года на первичную проверку соответствия системы сертифицированным стандартам. При вторичных проверках, конечно, этот период сократился. Основным направлением в решении данной задачи является разработка наименьшего необходимого количества требований к ПО при процессе аттестации операционных систем. Аналогично можно рассмотреть данные действия к гипервизору.

### 1.4.6 Системы хранения данных

Уровень сертифицированных в соответствии с требованиями информационной безопасности систем хранения данных не занимает должного уровня и оставляет желать только лучшего. На данном этапе единственной аттестованной системой является СУБД MSSQL. Мощные системы управления базами данных, такие как, DB2 или Oracle, необходимо поднимать свою категорию сертификации. При отсутствии документов, подтверждающих соответствие требованиям системы информационной безопасности, остается только полагаться на примененные средства защиты, которые не затрагивают внутренние механизмы упомянутых баз данных. Предложения по решению проблем защиты в этой области практически отсутствуют на рынке.

# Глава 2. Принципы защиты данных действующие в странах-членах Европейского союза

## 2.1 Риски по защите информационной безопасности в облачных вычислениях

Поскольку это мнение сфокусировано на операциях по обработке персональных данных в облачных вычислениях, далее будем рассматривать риски только связанные с этим. Большинство из этих рисков входят в две основные категории, а именно: отсутствие контроля над данными, и недостаточность информации относительно самой операции обработки (отсутствие прозрачности). Подробное рассмотрение этих риски облачных вычислений приведено далее.

### 2.1.1. Отсутствие контроля

Передав свои личные данные системе, управляемой провайдером облака, клиенты больше не могут обладать исключительным контролем этих данных и не могут принять какие-либо технические и организационные меры, необходимые для обеспечения доступности, целостности, конфиденциальности, прозрачности, изоляции, совместимости и защиты от вмешательства. Это отсутствие контроля может проявляться следующим образом:

Недоступность из-за отсутствия взаимодействия (вендора): если поставщик облака опирается на патентованную технологию, то может оказаться затруднительным для клиента перемещать данные и документы между различными облачными системами (переносимость данных) или для обмена информацией с лицами, которые используют облачные сервисы других поставщиков (функциональная совместимость).

Отсутствие целостности вызвано из-за совместного использования ресурсов: облака состоят из общих систем и инфраструктур. Облако поставщика обрабатывает персональные данные, поступающие из широкого круга источников. И с точки зрения данных субъектов и организаций может произойти конфликт интересов или возникнуть неясность цели.

Отсутствие конфиденциальности, а конкретно в запросах полиции напрямую к поставщику облака: личные данные, обрабатываемые в облаке, могут быть запрошены от представителей правоохранительных органов государств-членов ЕС и третьих стран. Существует риск того, что личные данные могут быть раскрыты (иностранных граждан) представителями правоохранительных органов без уважительной и законной основы.

Отсутствие способности вмешательства из-за сложности и динамики цепи аутсорсинга: облачные сервисы, предлагаемые одним поставщиком, могут изготавливаться путем комбинирования услуг из ряда других провайдеров облачных вычислений, которые могут быть динамически добавлены или удалены в процессе контракта клиента.

Отсутствие способности вмешаться (прав субъектов данных): провайдер облака не может обеспечить необходимыми мерами и инструментами для оказания помощи контроллеру для управления данными, например, доступ, удаление или исправление данных.

Отсутствие изоляции: облачные услуги могут использовать свой физический контроль над данным различных клиентов и связать персональные данные. Если администраторы обладали достаточными привилегированными правами доступа (с высокой степенью риска ролей), они могли бы взять это под контроль.

### 2.1.2.Отсутствие прозрачности

Недостаточная прозрачность операций облачного сервиса при обработке информации представляет опасность для контроллеров. А также для субъектов данных, потому что они не могут знать о потенциальных угрозах и рисках, и поэтому не могут принять меры, которые они сочтут необходимыми.

Некоторые потенциальные угрозы могут возникать в контроллере из-за того, что:

Технологическая цепочка проходит с участием нескольких процессоров и субподрядчиков.

Личные данные обрабатываются в различных географических районах, в рамках Европейского Экономического Пространства (ЕЭП). Это непосредственно влияет на права, применимые к любым спорам по защите данных, которые могут возникнуть между пользователем и поставщиком.

Личные данные передаются в третьи страны за пределами ЕЭП. Трети страны могут не иметь возможность обеспечивать адекватный уровень защиты данных и ее передача не могут гарантировать безопасность передачи данных путем принятия соответствующих мер (например, стандартных статей договора или обязательных корпоративных правил) и, следовательно, могут быть незаконными.

Это риски, о которых клиенты облачных сервисов, чьи персональные данные обрабатываются в облаке, должны быть оповещены (Существующее требование для всех контроллеров попадающие под Директиву о защите данных 95/46/ЕС). Учитывая потенциальные сложности цепочки обработки в среде облачных вычислений, с тем чтобы гарантировать справедливое рассмотрение прав в отношении субъекта данных (статья 10 Директивы 95/46/ЕС), контроллеры должны также, как это предусмотрено надлежащей практикой, представить дополнительную информацию, касающуюся (суб-) процессоров предоставления облачных сервисов.

## 2.2. Правовая основа

### 2.2.1. Структура защиты данных

Директива 95/46/ЕС о защите данных - соответствующая законодательная база. Эта Директива применяется в каждом случае, когда личные данные обрабатываются в результате использования вычислительных услуг облака. Электронная Директива Конфиденциальности 2002/58/EC (в редакции от 2009/136/EC) применяется при обработке персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи общего пользования (операторов связи) и, следовательно, очень важна, если такие услуги предоставляются посредством облачных решений.[[13]](#footnote-14)

### 2.2.2. Применяемы правовые нормы

Критерии для установления применимости законодательства содержатся Директивы 95/46/ЕС, в которой говорится о применении закона к контроллерам[[14]](#footnote-15) с одним или более учреждений в рамках ЕЭП, а также закон, регламентирующий контроллеры, которые находятся за пределами ЕЭП, но используют оборудование на обработку персональных данных, расположенное в рамках ЕЭП.[[15]](#footnote-16)

В первом случае, фактором вызывающим применение законодательства ЕС для контроллера является расположение его учреждения и осуществляемой ей деятельности в соответствии со статьей 4.1.(а) Директивы, в зависимости от типа модели облачных сервисов. Действующим законодательством является закон страны, в которой устанавливается контроллер договаривающихся сторон о предоставлении облачных услуг, а не место, в которой провайдеры облачных вычислений расположены.

Если контроллер устанавливается в различных государствах-членах ЕС, обработка данных в рамках своей деятельности в этих странах, будет правом каждого из государств-членов ЕС, в которых эта обработка происходит.

Статья 4.1.(c) гласит, как законодательство о защите данных применяется к контроллерам, учреждения которых расположены не в ЕЭП, но которые используют автоматизированное или не автоматизированное оборудования, расположенное на территории государств-членов ЕС, за исключением случаев использования в целях транзита. Это означает, что, если облако клиента будет установлено за пределами ЕЭП, но комиссия облачных услуг расположен в ЕЭП, то поставщик экспортирует законодательства защиты данных клиента.

### 2.2.3. Обязанности и ответственности сторон

Как указывалось ранее, облачные вычисления включают в себя целый ряд различных игроков. Важно оценить и уточнить роль каждого из этих игроков для того, чтобы установить их конкретные обязательства в отношении действующего законодательства о защите данных.

В первую очередь роль контроллера является определить, кто несет ответственность за соблюдение правил защиты данных, и как субъекты данных могут осуществлять свои права на практике. Другими словами: распределить ответственность. Эти два главных критерия отвечают за соблюдение и распределение ответственности и должны быть учтены заинтересованными сторонами в этом вопросе на протяжении всего времени.

#### 2.2.3.1 Клиент и провайдер в облаке

Клиент определяет конечную цель обработки и принимает решение об аутсорсинге этой обработки и делегации всех или части деятельности по обработке для внешней организации. Следовательно, клиент действует как контроллер данных. Директива определяет контроллер как "физическое или юридическое лицо, государственный орган, учреждение или любой другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных". Клиент, как контроллер, несет ответственность за соблюдение защиты данных законодательством. Пользователь облака может указать провайдерам облачных услуг на методы и технические или организационные меры, которые будут использоваться для достижения целей управления.

Провайдером облачных услуг является лицо, оказывающее услуги облачных вычислений в различных формах, что обсуждалось выше. Когда поставщик облака предоставляет средства и платформу, действуя от имени клиента, поставщик рассматривается как процессор данных, т.е. в соответствии с Директивой 95/46/ЕС "физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который самостоятельно или совместно с другими, обрабатывает персональные данные от имени контроллера".

На самом деле, могут быть ситуации, в которых поставщик облачных услуг может рассматриваться, либо как совместно с контроллером, либо в качестве контроллера в зависимости от конкретных обстоятельств. Например, это может быть в случае, когда провайдер обрабатывает данные для своих собственных целей.

Следует отметить, что даже в сложных средах обработки данных, где контроллеры играют важную роль в обработке персональных данных, соблюдение правил защиты данных и ответственность за возможное нарушение этих правил должно быть четко выделено для того, чтобы избежать снижения защиты личных данных. Или при "негативном конфликте компетенций" возникают пробелы, из-за чего обязательства или права, вытекающие из Директивы, не обеспечиваются какой-либо из сторон.

В текущем сценарии облачных вычислений, клиенты услуг облачных вычислений могут не иметь возможности для переговоров по контрактным условиям использования облачных сервисов, поэтому стандартизированные предложения являются характерной чертой многих услуг облачных вычислений. Тем не менее, в конечном счете это клиент принимает решение о распределении части или совокупность операций по переработке к облачным сервисам для конкретных целей; роль поставщика облачных услуг - подрядчик по отношению к клиенту, который является ключевым моментом в этом случае. Дисбаланс в условии договора между небольшим контроллером в отношении крупных поставщиков услуг не должен рассматриваться в качестве оправдания для контроллера при принятии положений и условий договора, которые не являются пунктами закона о защите данных[[16]](#footnote-17). По этой причине, контроллер должен выбрать поставщика облачных услуг, который гарантирует соблюдение законодательства о защите данных. Особый акцент должен быть сделан на особенностях соответствия с условиями договора - они должны включать в себя набор стандартных гарантий защиты данных, также гарантии на дополнительные механизмы, которые могут оказаться непригодными для облегчения должной осмотрительности и ответственности.

Провайдеры облака (как процессоры) обязаны обеспечить конфиденциальность. Директива 95/46 ЕС гласит о том, что: "Любой человек, действующий под руководством контроллера или процессора, в том числе сами процессоры, которые имеют доступ к персональным данным, не должны обрабатывать их, за исключением команд контроллера, если он не требуется сделать это по закону". Доступ провайдера к данным во время его предоставления услуг также принципиально регулируются требованием соблюдать положения статьи Директивы.

Процессоры должны принимать во внимание тип облака в вопросе (государственные, частные, общественные или гибридные - IaaS, SaaS или PaaS) и вид услуги по контракту с клиентом. Процессоры отвечают за принятие мер безопасности в соответствие с нормами законодательства ЕС. Процессоры должны также оказывать поддержку и помощь контроллеру в соблюдении прав (осуществлении) субъекта данных.

#### 2.2.3.2. Субподрядчики

Услуги облачных вычислений могут повлечь за собой участие в контракте ряда сторон, которые выступают в качестве процессоров. Это стандартная процедура для дополнительных суб-процессоров, которые затем получают доступ к персональным данным. Также процессоры, предоставляющие услуги субподряда, обязаны сделать доступной для клиента информацию, в которой подробно указаныусловия заключения субподряда, характеристика текущих или потенциальных субподрядчиков и гарантия того, что эти организации предлагают услуги облачных вычислений в соответствии с Директивой 95/46/ЕС.

Все соответствующие обязательства должны применяться к суб-процессорам на основе контракта между поставщиком облака и субподрядчика, который отражает условия договора между клиентом облака и его провайдером. Множеством процессоров в случаях, когда процессоры могут иметь прямую связь с контроллером или работать в качестве субподрядчиков, где процессоры в качестве аутсорсинга выполняют только порученную часть работы. Ничто, связанное с организационными требованиями согласно Директиве, не мешает нескольким субъектам, обозначенным как процессоры или суб-процессоры, назначать соответствующие задачи путем разделения. Тем не менее, все они должны соблюдать указания контроллера при выполнении обработки информации[[17]](#footnote-18).

В таких случаях, обязательства и обязанности, вытекающие из законодательства о защите данных, должны быть изложены четко, а не разбросаны по всей цепочке процесса аутсорсинга или субподряда, в целях обеспечения эффективного контроля и четкого распределения ответственности за обработку информации.

Возможная модель гарантий, которая может быть использована для уточнения обязанностей и обязательств процессоров, выступающих в роли субподряда по обработке данных, впервые была введенарешением комиссии от 5 февраля 2010 года по стандартным статьям договора о передаче личных данных процессоров в учреждения третьих стран[[18]](#footnote-19). В этой модели субподряд на обработку допускается только с предварительным письменным согласием контроллера и с письменным соглашениемвсех участвующих в процессе субподрядчиков. В случаях невыполнения субподрядчиком своих обязательств по защите данных, на которые он дал письменное согласие, на основе договора виновная сторона несет за это полную ответственность перед контроллером. Для обеспечения необходимых гарантий, положения такого рода используются в любых договорных условиях между контроллером и поставщиком облачных сервисов, где последний намерен предоставлять услуги на основе субподряда.

Недавно комиссией по общим положениям о защите данных было предложено аналогичное решение относительно гарантий в ходе суб-обработки. Акты процессоры должны регулироваться контрактом или иными правовыми актами, связывающие процессор с контроллером и предусматривающие, в частности, что, наряду с другими требованиями, процессор пользуется услугами другого процессора только с предварительного разрешения контроллера.

Провайдер может подрядить сторонние организации для выполнения своей деятельностиисключительно только на основании согласия контроллера[[19]](#footnote-20). Данное согласие, как правило, заключается перед началом оказания услуг. В нем четко распределены обязанности для процессора, обязующие последнего сообщать клиенту о любых планируемых изменениях, о добавление или замене субподрядчиков. За клиентом все время остается право возразить против такого изменения или расторгнуть договор. В обязательство провайдера входит указать в данном соглашении всех субподрядчиков процесса. Кроме того, договор, отражающий условия договора между клиентом и провайдером, должен быть подписан между поставщиком облака и субподрядчиками. Договор должен содержать условия, касательно действий, возникающих в случае нарушения субподрядчиками условий. Это может быть организовано путем того, что процессор берет на себя ответственность перед контроллером за любые нарушения, вызванные любыми привлеченными подпроцессорами. Или путем создания в контракте третьей стороны-бенефициара в пользу контроллера, подписанным между процессором и суб-процессорами. Или также возможно, что эти контракты будут подписаны напрямую от имени контроллера данных, что позже войдет в основной договор, как его часть.

### 

### 2.2.4. Требования по защите данных в отношениях сторон

#### 2.2.4.1. Соблюдение основных принципов

Законность обработки персональных данных в облаке зависит от соблюдения основных принципов закона ЕС о защите данных, а именно: должна быть гарантирована прозрачность в отношении субъекта данных, спецификация и ограничения по цели должны быть соблюдены и персональные данные должны быть стерты, как только необходимость в них исчезает. Кроме того, должны быть приняты соответствующие технические и организационные меры для обеспечения адекватного уровня защиты данных и их безопасности.

**Прозрачность**

Принцип прозрачности имеет ключевое значение для справедливой и законной обработки персональных данных. Директива 95/46/ЕС обязывает клиента предоставить информацию о предмете данных, с информацией о его идентичности и цели обработки.Клиент должен также предоставить любую дополнительную информацию, такую как на получатели или категорию получателей данных, которые могут также включать процессоры и суб-процессоры[[20]](#footnote-21). Такая дополнительная информация необходима, чтобы гарантировать справедливое рассмотрение прав в отношении субъекта данных.

Прозрачность должна быть обеспечена также в отношениях между клиентом, поставщиком облака и субподрядчиками (если таковые имеются). Клиент способен только дать оценку законности обработки персональных данных в облаке, если поставщик информирует клиента обо всех соответствующих вопросах.Контроллер, рассматриваемый привлечение услуг облака, должен внимательно проверить условия оказания услуг облачных вычислений, оценить их с точки зрения защиты данных.

Прозрачность в облаке означает, что для клиента необходимо быть в курсе всех субподрядчиков предоставляющих содействие соответствующей услуги облака, а также расположение всех центров обработки данных (ЦОД), где персональные данные могут быть обработаны.

Если предоставление услуги требует установки программного обеспечения на системе клиента (например, подключаемые модули браузера), провайдер облака должен, как это предусмотрено надлежащей практикой, информировать клиента об этом обстоятельстве и, в частности, о его последствиях влияющих на защиту данных, с точки зрения безопасности. И наоборот, клиент должен поднять этот вопрос, если он не будет уверен в достаточной степени облачных услуг.

**Определение и ограничение цели**

Принцип определения и ограничения цели требует, что личные данные должны быть собраны для определенных, явных и законных целей и не подвергались дополнительной обработке,расходящейся с этими целями[[21]](#footnote-22). Клиент должен определить цель обработки до момента самого сбора персональных данных и быть проинформированным о этом моменте. Клиент не должен передавать данные для других целей, которые не совместимы с оригинальными.

Кроме того, должно быть обеспечено, чтобы персональные данные не были (нелегально) обработаны для дальнейших целей поставщика облака или одного из его субподрядчиков. В типичном сценарии облако может легко включать большое количество субподрядчиков, поэтому риск обработки личных данных для дальнейших несовместимых целей должен быть оценен как достаточно высокий. Для минимизации данного риска, договор между поставщиком облака и клиентом должен включать технические и организационные меры по снижению этого риска и предоставлять гарантии для протоколирования и аудита соответствующих операций обработки персональных данных, которые выполняются поставщиком облака или субподрядчиками. Если законодательство о защите данных нарушено, штрафы на поставщика или субподрядчика должны быть наложены в соответствии с условиями договора.

**Удаление данных**

В соответствии с Директивой 95/46/ЕС, персональные данные должны храниться в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это необходимо для целей, для которых данные были собраны илидля которых они обрабатывались[[22]](#footnote-23). Личные данные, которые больше не нужны, должны быть удалены или переведены в статусанонимных. Если эти данные не могут быть удалены из-за юридических правил хранения (например, налогового законодательства), доступ к этим личным данным должен быть заблокирован. Ответственность за удаление персональных данных, как только они перестают быть необходимыми в условиях спецификации и ограничения цели, возлагается на провайдера облачных вычислений.

Принцип стирания данных распространяется на персональные данные, независимо от того, хранятся на жестких дисках или других носителях (например, ленты с резервными копиями). Так как личные данные могут избыточно быть на разных серверах и в разных местах, поставщик должен обеспечить, чтобы каждый экземпляр стирался безвозвратно (т.е. предыдущие версии, временные файлы и даже фрагменты файла должны быть удалены).

Клиенты должны быть осведомлены о том, что данные журнала, содействующие контролю, например, хранения, модификации или уничтожения данных, могут также квалифицироваться, как персональные данные, связанные с человеком, который инициировал соответствующие операции обработки.

Безопасное стирание персональных данных требует, чтобы, либо носители должны быть уничтожены или размагничивается, либо личные данные удалялись эффективно через перезапись. Для перезаписи данных личного характера используются специальные программные средства, которые переписывают данные несколько раз и с использованием соответствующей признанной спецификацией.

Клиент должен убедиться, что облака провайдера обеспечивают безопасное стирание, в вышеуказанном смысле, и что контракт между поставщиком и клиентом содержит ясные указания по стиранию личной информации. То же самое относится и к контрактам между облачными провайдерами и субподрядчиков.

#### 2.2.4.2. Договорные гарантии отношений «контроллер» - «процессор»

Там, где клиенты решили принять договор об оказании услуг облачных вычислений, контроллеры обязаны выбрать процессор, предоставляющий достаточные гарантии в отношении технических и организационных мер по обеспечению безопасности мер, проводить регулирование обработки, и должны обеспечивать соблюдение этих мер[[23]](#footnote-24). Кроме того, они по закону обязаны подписать официальный контракт с поставщиком облачных сервисов, как указано в Директиве 95/46/ЕС. Согласно Директиве устанавливаются требования к договору или иному правовому акту, обязательно определяющего взаимосвязь между контроллером и процессором. В цели сохранения доказательств, часть договора или правового акта, касающегося защиты данных и требований к ней, а также касающегося технических и организационных мер должна быть в письменной или в другой эквивалентной форме[[24]](#footnote-25).

В договоре должны, как минимум, установить факт, что процессор должен конкретно следовать указаниям контроллера, и процессор должен осуществлять технические и организационные меры для адекватной защиты персональных данных.

Для обеспечения правовой определенности в договоре должны также быть изложены следующие вопросы:

1. Подробная информация о (степень и формы) инструкций клиента по отношению к поставщику, особенно в касательно применимых соглашений об уровне обслуживания (которая должна быть объективной измеримой) и соответствующих санкций (финансовых или иных, включая возможностьподать в суд на поставщика в случае несоблюдения).
2. Спецификация мер безопасности:провайдер облака должен соответствовать всем требованиям, в зависимости от рисков, связанных с обработкой и характером данных, которые должны быть защищены. Имеет большое значение, какие конкретные технические и организационные меры указаны (такие меры будут разобраны ниже). Это рассматривается без ущерба при применении более жестких мер, если таковые могут быть предусмотрены национальным законодательством клиента.
3. Предмет и временные рамки облачных сервисов, предоставляемых провайдером облака; степень, характер и цели обработки персональных данных облачных услуг, а также типы обрабатываемых личных данных.
4. Необходимо указывать, какие условия для возвращения и разрушения (персональных) данных будут применяться. Кроме того, необходимо обеспечить, чтобы личные данные стирались безопасно и по просьбе клиента облака.
5. Включение пункта о конфиденциальности обязует соблюдение ее как провайдером на облаке, так и всех сотрудников сервиса облачных вычислений, которые смогут получить доступ к данным. Только уполномоченные лица могут получить доступ к данным.
6. Обязательство со стороны провайдера для поддержки клиента в содействии реализации прав субъектов данных для доступа, исправления или удаления своих данных.
7. В контракте должно быть конкретно установлено, что провайдер облака не имеет права сообщать данные третьим лицам, даже в целях хранения, если привлечение субподрядчиков не предусмотрено в договоре. В таких случаях, договор должен указать, что именно субподрядчикам может быть поручено на основе согласия, которые обычно задается контроллером в соответствии с четкими обязанностями процессора для информирования контроллера о любых планируемых изменениях в этой связи. За контроллером всегда сохранением возможность возразить против такого изменения или расторгнуть договор. В обязанности провайдера входит предоставление всей необходимой информации обо всех задействованных в процессе субподрядчиков (например, указать все в общественном цифрового регистре).Необходимо убедиться, что контракты между поставщиком облака и субподрядчиками отражают условия договора между клиентом облака и его провайдером (то есть, чтобысуб-процессоры исполняли те же договорные обязанности, чтопровайдер облака). В частности, необходима гарантия, что поставщик облака и все субподрядчики действуют только по поручению клиента облака. Вся цепочка ответственности должна быть предельно ясно отражена в договоре: сформулированы все обязательства, сформулированы международные переводы.
8. В случае любого нарушения данных, которое влияет на данные пользователя, провайдеру необходимо немедленно уведомлять клиента облака об этом.
9. В обязанность облачных сервисов входит предоставление списка мест, в которых данные могут быть обработаны.
10. Также в договоре должны быть изложены права контроллера по мониторингу процесса и соответствующие обязательства облачных сервисов к сотрудничеству в этом деле.
11. Следует установить в договоре, что поставщик облака должен сообщить клиенту о соответствующих изменениях, касающихся данных облачных сервисов, например, таких как осуществление внедрения дополнительных функций.
12. Договор должен предусматривать регистрацию и проверку соответствующих операций обработки персональных данных, которые выполняются поставщиком облака или субподрядчиком.
13. Уведомление клиента о любых юридически обязательных запросах, касательно раскрытия персональных данных правоохранительным органом, если иное не запрещено, например, запрет в соответствии с уголовным кодексом - сохранять конфиденциальность расследования правоохранительных органов.
14. Общие обязательства со стороны провайдера - дать гарантию того, что организация его внутренней обработки данных и механизмы (а также его суб-процессоров, если таковые имеются) соответствуют действующим национальным и международным правовым требованиям и стандартам.

В случае нарушений прав контроллером, любое лицо, потерпевшее ущерб в результате незаконной обработки, имеет право на получение компенсации от контроллера за нанесенный ущерб. Если процессоры используют данные для других целей или сообщают о них или используют их таким образом, что нарушают контракт, они также должны рассматриваться как контроллеры, и нести ответственность за нарушения, в которых они лично участвовали.

Следует отметить, что во многих случаях, провайдеры облачных сервисов предлагают стандартные услуги, и контракты для обработки персональных данных, которые клиенты должны подписать, излагаются в стандартной форме. Дисбаланс в условии договора между небольшим контроллером в отношении крупных поставщиков услуг не должен рассматриваться в качестве оправдания для контроллера при принятии положений и условий договора, которые не являются пунктами закона о защите данных

#### 2.2.4.3. Технические и организационные меры по защите и безопасности данных

В Директиве 95/46/ЕС описана полная ответственность клиента облака (выступающегов качестве контроллеров данных)по выбору облачных услуг, реализующих адекватные технические и организационные меры безопасности для защиты персональных данных с возможностью демонстрации подотчетности.

В дополнение к основной цели безопасности - доступности, конфиденциальности и целостности, также должно уделено внимание по защите данных в целях прозрачности, изоляции, способности вмешательства, подотчетности и портативности. Далее будут представлены более конкретно перечисленные выше главные цели[[25]](#footnote-26).

**Доступность**

Обеспечение доступности означает предоставление своевременного и надежного доступа к персональным данным.

Однаиз серьезных угроз доступности в облаке - случайная потеря подключения к сетимежду клиентом и поставщиком или производительным сервером, вызванная вредоносными действиями таких, как (распределенный) отказ в обслуживании, (DoS)атак. Другие риски включают в себя наличие случайногоаппаратногосбоя как в сети, так и в обработке данных в облаке и систем хранения данных. Так же риски связаны со сбоями питания и другими проблемами инфраструктуры.

Контроллеры данных должны убедиться, что провайдер облака принял разумные меры, чтобы справиться с риском нарушения, такие как резервное хранениессылок в сети Интернет, избыточное хранение и эффективное резервное копирования данных механизмов.

**Целостность**

Целостность может быть определена как свойство, которое удостоверяет подлинность данных,и отвечает за то, что с ними не происходило злонамеренных или случайных изменений во время обработки, хранения или передачи. Понятие целостности может быть распространено и на ИТ-систем, и требует, чтобы обработка персональных данных в этих системах оставалась неизменной.

Определение изменений в персональных данных может быть достигнуто путем криптографических механизмов аутентификации, таких как коды аутентификации сообщений или подписей.

Вмешательство в целостности ИТ-систем в облаке может быть предотвращено или обнаружено с помощью системы /предотвращения вторжений (IPS / IDS). Это особенно важно в открытых типах сетях, в которых облака обычно работают.

**Конфиденциальность**

В облачной среде, шифрование может внести значительный вклад в конфиденциальностьличных данных, если все сделано правильно, хотя оно не делает персональные данные необратимо анонимными[[26]](#footnote-27). Шифрование личных данных следует использовать во всех случаях, когда статус данных можно описать как «в пути» и "в покое"[[27]](#footnote-28). В некоторых случаях (например, службы хранения IaaS) клиент не может полагатьсяна шифрование, предлагаемое облаком услуг, но может выбрать тип шифрования личных данных перед отправкой их в облако. Шифрование данных в состоянии покоя требует особого внимания к управлению криптографическим ключом, так как безопасность данных, в конечном счете, зависит от конфиденциальности ключей шифрования.

Связь между поставщиком облака и клиентом, а также между центрами обработки данных должна быть зашифрована. Удаленное управление облачной платформой должнопротекать только по защищенному каналу связи. Если клиент планирует не только хранение, но и дальнейшую обработку персональных данных в облаке (например, поиск баз данных для записи), он должен иметь в виду, что шифрование не может быть обеспечено при обработке данных (за исключением очень специфических вычислений).

Дополнительные технические меры, направленные на обеспечение конфиденциальности, включают механизмы авторизации и строгой аутентификации (например, двухфакторная аутентификация). Договорные положения должны также налагать обязательства по соблюдению конфиденциальности на клиентов, поставщиков облачных услуг и субподрядчиков.

**Прозрачность**

Технические и организационные меры должны поддерживать прозрачность, чтобы позволить обзор процесса. Данное свойство уже было рассмотрено выше.

**Изоляция (цель ограничения)**

В облачных инфраструктурах ресурсы, такие как хранение, память и сеть - являются общими для многих арендаторов. Это создает новые риски для данных, подвергая их к раскрытию и обработке в незаконных целях.Защита цели «изоляции» предназначена для решения этой проблемы и способствует гарантии, что данные не будут использоваться за пределами своего первоначального назначения, а также для поддержки конфиденциальности и целостности

Во-первых, достижение изоляциитребует адекватного управления правами и ролями для доступа к личным данным, которые рассматриваются на регулярной основе. Реализации роли с чрезмерными привилегиями следует избегать (например, ни один пользователь или администратор не должны иметь право доступа ко всему облаку). В более общем плане, администраторы и пользователи должны только получить доступ к информации, необходимой для их законных целей (принцип наименьших привилегий).

Во-вторых, изоляция также зависит от технических мер, таких как упрочнение гипервизоров и надлежащее управление общими ресурсами, если виртуальные машины применяются для совместного использования физических ресурсов между различными клиентами.

**Способность вмешательства**

Директива 95/46/ЕС дает субъекту данных права доступа, исправления, удаления, блокировки и возражения[[28]](#footnote-29). Клиент облака должен убедиться, что провайдер облака не накладывает технических и организационных препятствий к этим требованиям, в том числе в случаях, когда данные обрабатываются в дальнейшем субподрядчиками.

Договор между клиентом и поставщиком должен предусматривать, что поставщик облака обязан оказать поддержку клиенту в содействии реализации прав субъекта данных и гарантировать, что тоже самое будет в отношенииего к любым субподрядчикам

**Портативность**

В настоящее время большинство облачных провайдеров не используют стандартных форматов данных и интерфейсов служб для содействия совместимости и переносимости между различными провайдерами облака. Если клиент решает мигрировать из одного облака провайдера к другому, отсутствие этого взаимодействия может привести к невозможности или, по крайней мере, к трудности передать личные данные клиента на облако нового провайдера (так называемого вендора). Тоже самое справедливо и для услуг, на платформе которых развернулся клиент, и которое ему предложил первоначально поставщик облака (PaaS). Клиент должен проверять, как поставщик гарантирует мобильность данных и услуг перед заказомоказания услуг облачных сервисов.

**Подотчетность**

В информационных технологиях подотчетность может быть определена как возможность установить, какие лица сделали в определенный шаг в определенный момент времени в прошлом и как. В области защиты данных часто требуется более широкое значение и характеризуется способностью стороны продемонстрировать, что они приняли соответствующие меры для обеспечения того, чтобы принципы защиты данных были выполнены.

Подотчетность в ИТособенно важна для того, чтобы расследовать нарушения прав личных данных, где клиенты, поставщики и суб-подрядчики могут иметь некую степень эксплуатационной ответственности. Способность платформы облака кобеспечения надежного и всеобъемлющего механизма мониторинга ведения журналов имеет первостепенное значение в этом отношении.

Кроме того, облачные провайдеры должны документально подтверждать надлежащие и эффективные меры, которые обеспечивают результаты защиты принципов данных, изложенных выше. Процедуры, обеспечивают идентификацию всех операций обработки данных, отвечают на запросы доступа, распределение ресурсов, в том числе назначение для защиты данных лиц, которые несут ответственность за организацию защиты данных соответствия, или независимые процедуры сертификации, которые являются примерами таких мер. Кроме того, данные контроллеры должны гарантировать, что они готовы продемонстрировать создание необходимых мер для компетентного надзорного органа по запросу[[29]](#footnote-30).

### 2.2.5. Международные передачи

Директива 95/46/ЕС предусматривает свободный поток персональных данных в страны, расположенные за пределами ЕЭП, только если эти страны или получатель обеспечивают адекватный уровень защиты данных. В противном случае конкретные гарантии должны быть введены в действие контроллера и его со-контроллеровили процессоров. Однако, облачные вычисления чаще всего основаны на полном отсутствии стабильного расположения данных в сети облачных вычислений. Данные могут быть в одном центре обработки данных в 2 часа дня, а в 4 вечера уже находиться в другом конце света. Поэтому клиент редко в состоянии имеет возможность знать, в реальном времени, где находятся, хранятся или передаются данные. В этом контексте, традиционные правовые акты, обеспечивающие базу для регулирования передачи данных за пределами ЕС третьим странам, не обеспечивает адекватную защиту, имеют ограничения.

#### 2.2.5.1. SafeHarbor и отвечающие требованиям страны

SafeHarbor (закон), положение закона или постановление, которое уменьшает или устраняет ответственность участника в соответствии с законом, при условии, что партия выполняет свои действия в добросовестности или в соответствии с определенными стандартами.

Адекватность результатов, в том числе SafeHarbor, ограничены в отношении географического охвата, и, следовательно, не покрывают все трансферы внутри облака. Трансферы в организации США в соответствии с принципами могут происходить законно в соответствии с законодательством ЕС, так как организации получателя обеспечены адекватным уровнем защиты передаваемых данных.

Однако, единственная самостоятельная сертификация с SafeHarbor не может считаться достаточной при отсутствии надежных исполнительных принципов защиты данных в облачной среде. Кроме того, Директива ЕС требует, чтобы договор должен быть подписан контроллером в отношении процессоров целях обработки, что подтверждается в FAQ 10 (часто задаваемые вопросы) EU-US Safe Harbor Framework документах. Такой договор определяет процессы обработки, будет осуществлять любые меры, необходимые для обеспечения того, чтобы данные хранились в безопасности. Различные национальные законодательства могут иметь дополнительные требования.

Компании, экспортирующие данные, не должны просто полагаться на заявления поставщиков услуг, утверждающих, что у них есть свидетельство Safe Harbor. Напротив, компания экспортирующая данные должна получить доказательства того, что это свидетельство существует и запросить доказательства того, что их все принципы, применяемые к защите данных, соблюдаются. Особенно это важно в отношении информации, предоставляемой клиентами, пострадавших в результате обработки данных.

Также клиент должен проверять составленные стандартные контракты по предоставление облачных услуг на соответствие национальным требованиям в отношении обработки данных. Национальное законодательство может потребовать выдать запрос, который будет определен в контракте, результат которого содержит сведения и другие данные по суб-процессам, и отслеживанию данных. Обычно облачные услуги не предлагают клиенту такую информацию –собственные обязательства по Safe Harbor не могут заменить гарантиями выше, даже когда это требуется национальным законодательством. В таких случаях экспортеру рекомендуется использовать другие правовые документы, такиекак стандартные статьи договора или BCR (обязательные корпоративные правила).

Принципы Safe Harbor сами по себе также не могут гарантировать экспортеру данных, что все средства необходимые для обеспечения того, чтобы были применены соответствующие меры безопасности в облачных сервисах в США, которые в свою очередь национальное законодательство может запросить на основе Директивы 95/46/EC. С точки зрения безопасности данных вычислительного облака поднимаются несколько конкретных угроз безопасности в облаке: потеря управления, небезопасное или неполное удаление данных, недостаточность сквозной проверки или изоляция сбоев, которые не получили достаточного освещения существующими принципами Safe Harbor по безопасности данных[[30]](#footnote-31). Таким образом, дополнительные гарантии для защиты данных могут быть развернуты, например, путем включения опыта и ресурсов третьих лиц, которые способны к оценке адекватности облачных услуг через различные инструменты аудита, стандартизации и сертификации. По этим причинам было бы целесообразно дополнить обязательство импортера данных в соответствии Safe Harbor с дополнительными гарантиями и учетом специфики облака.

#### 2.2.5.2. Исключения

Исключения, предусмотренные Директивой ЕС 95/46, позволяют экспортерам данных передавать данные из ЕС без предоставления дополнительных гарантий. Тем не менее, считается, что исключения должны применяться только там, где переводы не являются повторяющимися, массивными или структурными[[31]](#footnote-32).

На основе такого мнения, это почти невозможно рассчитывать на исключения в контексте облачных вычислений.

#### 2.2.5.3. Стандартные условия договора

Стандартные условия договора, приняты комиссией ЕС с целью разработки международной передачи данных между двумя контроллерами или одним контроллера и процессором, основанной на двустороннем подходе. Когда облако поставщика считается процессором, типовые положения 2010/87/EC (решение комиссии) являются инструментом, которые можно использовать между процессором и контроллером в качестве основы для среды облачных вычислений, чтобы предложить адекватные меры в контексте международных переводов.

В дополнение к стандартным договорным положениям, необходимо добавить, что облачные провайдеры могли бы предложить клиентам положения, которые основываются на своем прагматичном опыте, если он не противоречит, прямо или косвенно стандартам статьи договора, одобрен комиссией и не нарушает основных прав и свободу субъектов данных. Тем не менее, компания не может убрать или изменить стандартные условия договора, не подразумевая, что положениябудет уже не "стандартными".

Когда поставщик облака выступает в качестве процессора, установленного в ЕС, ситуация может быть более сложной, поскольку типовые положения относятся, в общем, только на передачу данных от контроллера ЕС к процессору, который располагается на территории ЕС.

Что касается договорных отношений между процессором(не из ЕС) и суб-процессором, оформляется письменное соглашение, которое накладывает те же обязанности на суб-процессор, какие установлены и на процессор в типовых положениях.

#### 2.2.5.4. Обязательные корпоративные правила на пути к глобальному подходу

BCR составляют кодекс поведения для компаний, которые передают данные в пределах их группы. Таким решением также будут обеспечены облачные вычисления, когда поставщик является процессором. Действительно, в настоящее время ведутся работы над BCRs для процессоров, которые позволят передачу в рамках группы с пользой для контроллеров без требования подписания контракта между процессором и суб-процессором в учете на одного клиента.

Такие BCR для процессоров позволят клиенту провайдера доверить свои личные данные в процессор, будучи уверенным, что данные, передаваемые в пределах сферы деятельности провайдера, получат адекватный уровень защиты.

**Заключение**

В ходе работы было разобрано понятие информационной безопасности.

В нашем случае, под «информационной безопасностью» мы будем понимать степень защиты информации и обеспечивающие ее существование инфраструктуры от нежелательного (случайного и специального) воздействия, которое в дальнейшем способно нанести неприемлемый ущерб участникам информационных отношений.

Выделены следующие типы угроз для информации:

* Искусственные:
* непреднамеренные угрозы,
* преднамеренные угрозы.
* Естественные:
* неправильное хранение,
* кража компьютеров и носителей,
* форс-мажорные обстоятельства,
* пожары, наводнения, ураганы, удары молний и другие стихийные бедствия и явления, которые не зависят от человека.

Для обеспечения информационной безопасности используют три основных метода:

* правовые,
* организационно-технические
* экономические.

Также в ходе работы приведен подробный разбор структуры работы облачных вычислений, а именно: характеристики облачных сервисов, основные преимущества и недостатки использования данной технологии.

Облака по своему предназначению делятся на три основных вида:

1. *SaaS -* "Softwareas as Service" *- программное обеспечение как услуга;*
2. *PaaS -* "Platformas as Service" *платформакакуслуга;*
3. *IaaS -* "Infrastructureas as Service "*инфраструктуракакуслуга.*

Преимущества использования технологии облачных вычислений:

* Недорогие компьютеры для пользователей.
* Увеличенная производительность пользовательских компьютеров.
* Уменьшение затрат и увеличение эффективности IT инфраструктуры.
* Меньше проблем с обслуживанием и затрат на приобретаемое программное обеспечение.
* Увеличение доступных вычислительных мощностей.
* Неограниченный объем хранимых данных.
* Совместимость с большинством операционных систем.
* Улучшенная совместимость форматов документов.
* Простота совместной работы группы пользователей.
* Повсеместный доступ к документам.
* Всегда самая последняя и свежая версия. В "облаке" всегда находится самая последняя и самая свежая версия программы или документа.
* Доступность с различных устройств.
* Дружелюбие к природе, экономное расходование ее ресурсов.
* Устойчивость данных к потере или краже оборудования.

Недостатки от использования:

* Постоянное соединение с сетью Интернет.
* Плохо работает с медленным Интернет-доступом.
* Программы могут работать медленнее чем на локальном компьютере.
* Не все программы или их свойства доступны удаленно.
* Безопасность данных может быть под угрозой.

На основании статьи А.П.Баранова «Можно ли защитить в облаке конфиденциальную информацию?» процесс работы облачных сервисов разделен на 6 этапов, в каждом из которых выделены проблемы защиты:

1) Аппаратные компоненты центра обработки данных.

2. Телекоммуникационная составляющая доступа к ресурсам центра обработки данных.

3. Пользователи и их программно-аппаратное обеспечение.

4. «Средний» (middleware) слой центра обработки данных.

5. Прикладные сервисы.

6. Системы хранения данных (СУБД).

При анализе ситуации по обеспечению безопасности информации в странах-членах Европейского союза были разобраны риски по защите информации. Большинство из этих рисков входят в две основные категории, а именно: отсутствие контроля над данными, и недостаточность информации относительно самой операции обработки (отсутствие прозрачности).

Приведен подробный анализ правовой структуры применяемой к участникам информационных отношений. В ходе анализа разобраны: правовые нормы, обязанности и ответственности сторон, требования по защите данных. В последнем приведены технические и организационные меры по защите и безопасности данных, которые включают в себя контроль таких пунктов как:

* Доступность;
* Целостность;
* Конфиденциальность;
* Прозрачность;
* Изоляция (цель ограничения);
* Способность вмешательства;
* Портативность;
* Подотчетность.

# Библиографический список

1. Directive 95/46/EC ofthe European Parliamentandof the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
2. Directive 2002/58/EC of the European Parliament and of the Councilof 12 July 2002concerning the processing of personal data and the protection of privacy in the electroniccommunications sector (Directive on privacy and electronic communications)
3. Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002)
4. Доктрина информационной безопасности РФ 9 сентября 2000 г.
5. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных»
7. Ярочкин В.И. Информационная безопасность. Учебник для вузов.– М.: Академический Проект, Мир, 2004. – 544 с.
8. Левин В.К. Защита информации в информационно-вычислительных cистемах и сетях. Программирование. - 1994. - N5. - с. 5-16.
9. Баранов А.П «Можно ли защитить в «облаке» конфиденциальную информацию?» \\ Системы высокой доступности, 2012. Т. 8. № 2. C. 12—15
10. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. – 544 с.
11. Белогрудов В.М. Облачные вычисления - достоинства и недостатки \\ http://www.smart-cloud.org/sorted-articles/44-for-all/96-cloud-computing-plus-minus. 03.03.2012
12. Кондрашин М.С. Безопасность облачных вычислений \\ <http://www.pcmag.ru/solutions/detail.php?ID=38248>. 15.02.2010
13. Мельников В.И. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 1997. – с. 123 – 128.
14. Угрозы информационной безопасности \\ [http://www.internet-technologies.ru/articles/article\_1147.html. 3.10.2007](http://www.internet-technologies.ru/articles/article_1147.html.%203.10.2007)
15. Интернет-Университет Информационных Технологий \\ <http://www.intuit.ru/department/security/secbasics/1/secbasics_1.html>
16. Хореев П.В. Методы и средства защиты информации в компьютерных системах. – М.: издательский центр "Академия", 2005. – с. 205.
17. Фатьянов А.А. Концептуальные основы обеспечения безопасности на современном этапе \\ Безопасность информационных технологий – 1999 - №1. С.26-40.
18. Приходько А.Я. Словарь-справочник по информационной безопасности. М.: СИНТЕГ, 2001. 124 с.
19. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптографическая деятельность в США XVIII-XIX веков. \\ Защита информации. Конфидент. №6, 2004, с.68-74.
20. Тейер Т., Липов М., Нельсон Э. Надежность программного обеспечения. - Пер. с англ. - М.: Мир, 1981.
21. Липаев В.В. Надежность программных средств. - М.: Синтег, 1998.
22. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. О развитии криптографии в XIX веке // Защита информации. Конфидент. №5, 2003, с.90-96.
23. [www.ec.europa.eu/justice](http://www.ec.europa.eu/justice)
24. [www.enisa.europa.eu](http://www.enisa.europa.eu)

1. Доктрина информационной безопасности РФ 9 сентября 2000 г [↑](#footnote-ref-2)
2. Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных» [↑](#footnote-ref-3)
3. Ярочкин В.И. Информационная безопасность. Учебник для вузов.– М.: Академический Проект, Мир, 2004. – 544 с. [↑](#footnote-ref-4)
4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. – 544 с. [↑](#footnote-ref-5)
5. Угрозы информационной безопасности \\ [http://www.internet-technologies.ru/articles/article\_1147.html. 3.10.2007](http://www.internet-technologies.ru/articles/article_1147.html.%203.10.2007) [↑](#footnote-ref-6)
6. Хореев П.В. Методы и средства защиты информации в компьютерных системах. – М.: издательский центр "Академия", 2005. – с. 205 [↑](#footnote-ref-7)
7. Приходько А.Я. Словарь-справочник по информационной безопасности. М.СИНТЕГ, 2001. 124 с. [↑](#footnote-ref-8)
8. Белогрудов В.М. Облачные вычисления - достоинства и недостатки \\ http://www.smart-cloud.org/sorted-articles/44-for-all/96-cloud-computing-plus-minus. 03.03.2012 [↑](#footnote-ref-9)
9. Фатьянов А.А. Концептуальные основы обеспечения безопасности на современно этапе \\ Безопасность информационных технологий – 1999 - №1. С.26-40. [↑](#footnote-ref-10)
10. Кондрашин М.С. Безопасность облачных вычислений \\ <http://www.pcmag.ru/solutions/detail.php?ID=38248>. 15.02.2010 [↑](#footnote-ref-11)
11. Баранов А.П «Можно ли защитить в «облаке» конфиденциальную информацию?» \\ Системывысокойдоступности, 2012. Т. 8. № 2. C. 12—15 [↑](#footnote-ref-12)
12. Тейер Т., Липов М., Нельсон Э. Надежность программного обеспечения. - Пер. с англ. - М.: Мир, 1981. [↑](#footnote-ref-13)
13. **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector** [↑](#footnote-ref-14)
14. Концепциюконтроллераможнонайтивстатье 2 Директивы, которуюпроанализировалив Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002) [↑](#footnote-ref-15)
15. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179\_en.pdf [↑](#footnote-ref-16)
16. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\_en.pdf [↑](#footnote-ref-17)
17. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\_en.pdf [↑](#footnote-ref-18)
18. <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> [↑](#footnote-ref-19)
19. Article 29 Working Party Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56 of 30 May 2002) [↑](#footnote-ref-20)
20. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-21)
21. Article 6(b) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-22)
22. Article 6(е) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-23)
23. Article 17(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-24)
24. Article 17(3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-25)
25. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-

    risk-assessment [↑](#footnote-ref-26)
26. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-27)
27. Article 8 of Directive 95/46/EC (e.g., health data) to the cloud or who are subject to specific legal obligations of

    professionalsecrecy [↑](#footnote-ref-28)
28. Article 12 and 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [↑](#footnote-ref-29)
29. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173\_en.pdf. [↑](#footnote-ref-30)
30. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-

    risk-assessment [↑](#footnote-ref-31)
31. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12\_en.pdf [↑](#footnote-ref-32)