ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДАННЫХ, ПРЕДСТАВЛЕННЫХ В ОБЛАЧНЫХ СЕРВИСАХ

Вишняков А.С.[1], Макаров А.Е.[2], Уткин А.В.[3], Зажогин С.Д.[4], Бобров А.В.[5]
Email: Vishniakov665@scientifictext.ru

[1]Вишняков Александр Сергеевич – ведущий инженер,
системный интегратор «Крастком»;
[2]Макаров Анатолий Евгеньевич – архитектор решений,
Российская телекоммуникационная компания «Ростелеком»,
г. Москва;
[3]Уткин Александр Владимирович – старший инженер,
Международный системный интегратор «EPAM Systems», г. Минск, Республика Беларусь;
[4]Зажогин Станислав Дмитриевич - старший разработчик,
Международный IT интегратор «Hospitality & Retail Systems»;
[5]Бобров Андрей Владимирович – руководитель группы,
группа технической поддержки,
Компания SharxDC LLC,
г. Москва

Аннотация: *в статье авторы выкладывают глубокий анализ существующих, на данный момент, решений задачи о безопасности данных в облачных системах. Проводится обзор литературных источников и направлений по решению безопасности облаков. В форме таблицы подана информация по поводу распределения ответственности по обеспечению безопасности между клиентом и поставщиком услуги.*

Проведен сравнительный анализ безопасности данных в известных облачных моделях, а также описываются альтернативные решения вопросов по безопасности, в зависимости от модели SaaS, PaaS или IaaS. На рис. 1 показаны наиболее актуальные угрозы для информационных баз, существующие на данный момент.

Рассматриваются ключевые элементы облачной системы, которые могут быть в опасности со стороны атак злоумышленников: гипервизор, руководитель виртуальной системой облаков, центр для обработки информационных данных, где расположена большая часть информации, которая является конфиденциальной, канал, который обеспечивает связь между потребителем облачных услуг, программное обеспечение, установленное на компьютере пользователя (прежде всего, интернет-браузер).

Показано, что на сегодняшний день вопросы по обеспечению защиты информационных данных, построению доверия пользователей по отношению к провайдерам, представляющим услуги в рамках облачных технологий, являются приоритетными в плане будущего развития облачных вычислений.

Ключевые слова: *облачные технологии, сервер, атака, безопасность, средства облачных технологий, хранилища данных, файловый хостинг, автоматизированные системы.*

ENSURING THE PROTECTION OF DATA PROVIDED IN CLOUD SERVICES

Vishniakov A.S.[1], Makarov A.E.[2], Utkin A.V.[3], Zazhogin S.D.[4], Bobrov A.V.[5]

[1]Vishniakov Alexandr Sergeevich – Lead System Engineer,
SYSTEM INTEGRATOR «KRASTCOM»;
[2]Makarov Anatoly Evgenevich – Solutions Architect,
ROSTELECOM INFORMATION TECHNOLOGY,
MOSCOW;
[3]Utkin Alexander Vladimirovich – Senior Engineer,
INTERNATIONAL SYSTEM INTEGRATOR EPAM SYSTEMS, MINSK, REPUBLIC OF BELARUS;
[4]Zazhogin Stanislav Dmitrievich – Senior Software Engineer,
International IT Integrator Hospitality & Retail Systems;
[5]Bobrov Andrei Vladimirovich – Team leader,
TECHNICAL SUPPORT GROUP,
SHARXDC LLC,
MOSCOW

Abstract: *in the article, the authors lay out a deep analysis of the existing, at the moment, solutions to the problem of data security in cloud systems. A review of the literature, and directions to address the safety of clouds. The table form contains information on the distribution of security responsibilities between the client and the service provider.*

A comparative analysis of data security in well-known cloud models has been conducted, and alternative solutions to security issues are described, depending on the SaaS, PaaS or IaaS model. In fig. 1, shows the most current threats to information databases that exist at the moment.
The key elements of the cloud system that may be at risk from malicious attacks are considered: hypervisor, virtual cloud system manager, information processing center, where most of the information is confidential, the channel that provides communication between the cloud service consumer, software installed on the user's computer (primarily an Internet browser).
It is shown that today the issues of ensuring the protection of information data, building user confidence in relation to providers of services within the framework of cloud technologies are priorities in terms of the future development of cloud computing.
Keywords: *cloud technologies, server, attack, security, cloud technology tools, data storage, file hosting, automated systems.*

УДК 331.225.3

Введение

Облачные технологии имеют большую популярность среди активных пользователей сети Интернет, поскольку предоставляют большой спектр услуг в плане многопользовательской структуры, легкости в работе, экономичности, а это, в свою очередь, способствует улучшению качества работы пользователей и влечет за собой популяризацию облаков на рынке ИТ услуг. Весьма важным аспектом является экономичность облачных технологий, что является доступным для различных слоев населения для хранения информационных данных. Некоторые предприятия используют для работы, которая требует временных вычислений, публичные облака вместо того, чтобы настраивать собственную внутреннюю инфраструктуру, это удобно в финансовом плане, расчет идет только за время использования. Необходимо помнить, что использование облачных технологий влечет за собой повышенные риски потери информации и, кроме того, возможность контроля ограниченная.

Изучение особенностей проведения облачных вычислений с позиции обеспечения безопасности информации можно структурировать следующим образом: сбережение данных у незаинтересованной стороны; возможность руководить и контролировать вопрос безопасности при необходимости; контроль за нарушениями в режиме реального времени; организация работоспособности облачных сервисов; решение вопроса подготовки квалификационных кадров по направлению организации безопасности облачных систем; регулярные инвестиции в развитие инфраструктуры безопасности облаков.

Если рассматривать публичное облако, то оно, как и множество других систем, которые функционируют в сети Интернет, может подвергаться атакам. Для облачных систем характерны следующие виды атак: стандартные атаки на программное обеспечение; атаки нацелены на клиента; сетевые атаки; атаки сосредоточены на серверы облака; реализация разноплановых угроз [3, 5].

Если успешно организована хакерская атака, то практически на каждый из элементов облака нависает угроза нарушения безопасности информации (целостность, приватность, конфиденциальность).

Важным аспектом при организации высокого уровня безопасности является передача частных данных незаинтересованной стороне, что обусловливает наличие дополнительных протоколов работы между потребителем и поставщиком необходимых услуг облачной системы. В связи с этим представляет интерес изучения известных подходов к защите информации при использовании облачных вычислений.

Анализ последних исследований и публикаций. Исследование по поду построения системы безопасности облачных сервисов, является весьма популярной в современном мире развития информационных технологий. Основные направления и пути будущих перспективных исследований облачных технологий детально изложены в работах Е.А. Боклачевой, И.В. Герасименко, Т. Димитракоса, В.А. Заславского, Н.А. Масловой, О.В. Мовчана, А.С. Паламарчук, Е.О. Савкова, Т.А. Степанова, Дж. Риза и многих других [3-6]. В статье И.В. Герасименко проведен обзор существующих облачных сервисов, приложений и их функциональных характеристик.

Если говорить о приоритетных направлениях развития высокого уровня безопасности облачных технологий, то невозможно не обратить внимание на лучших экспертов в этой сфере, а именно организацию – Security Alliance (CSA), которая выпустила и недавно усовершенствовала рекомендации которые необходимо учитывать при проведении оценки рисков в сфере облачных вычислений, а также организацию – Trusted Computing Group (TCG), которая является автором известных в среде использовании ИТ специалистов стандартов Trusted Storage, Trusted Network Connect (TNC) и Trusted Platform Module (TPM) [1].

Детальный анализ о работе облачных систем был проведен организацией CSA, результаты которого были изложены в документе "Top threats of Cloud Computing v 1.0" в котором наиболее полно и доступно описываются модель угроз и модель нарушителя. В названом документе, предельно ясно описано возможные нарушители для основных сервисных моделей таких как: SaaS, PaaS и IaaS, а также сформированы 7 направлений по которым возможны атаки [3].

Исследование литературных источников показало, что вопрос о разработке безопасности облачных сервисов – это сравнительно новое направление и требует дополнительных исследований с целью расширение возможностей для построения надежных облачных хранилищ [1-4].

Формулирование целей статьи (постановка задачи). Провести детальное исследование, существующих на данный момент решений задачи о безопасности данных в облачных системах.

Изложение основного материала исследования. Для успешной организации информационной безопасности облачной системы необходимо учитывать следующие элементы: подсистему, которая обеспечивает надежное хранение информации у клиента; подсистему которая организовывает безопасность в сети; подсистему обеспечения надежности виртуальных сред; подсистему которая позволяет организовать безопасную работу в центрах обработки данных. Необходимо отметить, что, как и в других подобных системах, предназначенных для защиты информации, говорить про успешно организованную безопасность облачной системы можно тогда, когда работа всех подсистем организованно на высшем уровне [2-4].

Для детального изучения вопроса исследования безопасности в облаках проанализируем, в частности, каждую из перечисленных выше подсистем.

Подсистема, которая обеспечивает надежное хранение информации у клиента может быть подвержена таким угрозам как – Cross-site-scripting (XSS), Phishing, вирусы, трояны это можно объяснить тем, что пользователи вынуждены работать с сервисом облачных вычислений используя интернет-браузер. Для того чтобы организовать безопасность информации на этом уровне необходимо на стороне клиента придерживаться выполнения наличия следующих элементов: антивирусные пакеты программ для защиты информации; средства позволяющие шифровать данные на диске; персональный брандмауэр, который будет находиться в ОС; интернет-браузер который правильно настроен с точки зрения безопасного подключения к сети [5-6].

Подсистему, которая организовывает безопасность в сети необходимо организовывать таким образом чтобы данные которые находятся в публичном облаке были в безопасности для этого нужно использовать специальный туннель виртуальной частной сети (VPN), он предоставляет возможность объединить клиента и сервер с целью получения публичных облачных услуг. VPN-туннель позволяет совершать безопасные соединения и кроме того пользователь имеет возможность использовать единое имя и пароль для входа к различным облачным ресурсам. VPN- соединение использует ресурсы Интернет, доступ к которым имеют все пользователи, для того чтобы организовать процесс передачи данных для публичных облаков. Описанный механизм возможно реализовать на практике с помощью режимов доступа с шифрованием с использованием двух ключей на базе протокола Secure Sockets Layer.

Подсистема обеспечения надежности виртуальных сред зависит от безопасности механизмов виртуализации. Если успешно реализована атака на гипервизор, то злоумышленник может в тайне, незаметно для систем защиты информации, которые функционируют в виртуальных машинах, совершать следующие действия: копировать блокировать информационный поток данных, который идет на различные устройства ((HDD, принтер, USB); читать и редактировать информацию на дисках виртуальных машин, следует отметить что эти действия будут возможны и при выключенных машинах, без участия их программного обеспечения. Для того чтобы решить описанную проблему необходимо защитить гипервизор для этого нужно разграничить права доступа к серверу виртуализации, это возможно сделать путем своевременной установки обновлений программного обеспечения среды виртуализации, а также нужно ограничить запуск программ [1, 2].

Диск виртуальной машины находится на SAN/NAS, в связи с этим становится актуальным вопрос о защите информационных данных виртуальных машин путем ограничение доступа к дискам машин с помощью сертифицированных средств защиты информации и специальными экранами, которые способны контролировать протоколы и другие элементы виртуальной инфраструктуры.

Если злоумышленник получит доступ к средствам администрирования, то он будет иметь возможность до редактирования данных, уничтожения, похищения и т.п., во всей сети виртуальной инфраструктуры. Чтобы избежать подобных случаев атак, необходимо защитить доступ к сети администрирования, серверам виртуальных машин, всевозможным средствам управления инфраструктурой.

Виртуальные машины, которые имеют один физический сервер, имеют возможность совершать обмен трафиком напрямую, не используя при этом сетевые коммутаторы, в этом случае использование межсетевых экранов не будет весьма эффективным, для успешного решения этой проблемы необходимо усовершенствовать существующие сертифицированные экраны и их перенос в виртуальную среду, кроме этого нужно еще создать специализированные средства защиты информации, которые смогут контролировать трафик внутри необходимого сервера. По сети репликации передаются сегменты их оперативной памяти, поэтому если злоумышленники во время атаки перехватят данные, то существует прямая угроза безопасности, отсюда следует что сеть репликации необходимо изолировать от других сетей и кроме того использовать сертифицированные VPN для канала репликации. Не нужно

рассчитывать на тривиальность структуры виртуальных машин поскольку это может привести к большим проблемам с безопасностью, а необходимо организовать процесс управления виртуальными машинами, таким образом, чтобы он был согласован с политикой безопасности организации [4].

Подсистема, которая позволяет организовать безопасную работу в центрах обработки данных (ЦОД), способна обеспечить безотказную работу системы на всех ее уровнях безопасности, надежности, доступности. Использование описанной технологии предоставляет возможность создавать резервные хранилища информации и при этом не терять функциональность информационной системы.

Для лучшего понимания организации безопасности облачных систем рассмотрим структуру ЦОД. Центр данных являет собою кластер серверов, главная цель создания которого состоит в том, чтобы повышать эффективность безопасности в плане физической и сетевой защиты. Объектами защиты в ЦОД можно назвать следующие элементы – оборудование, частная информация, программное обеспечение. Подсистема ЦОТ в своем составе имеет: видеонаблюдение; пожарную сигнализацию; систему контроля для управления доступом; систему для создания резервного копирования, восстановления информации; систему для защиты безопасности данных ЦОД, опишем каждую из перечисленных систем.

Наличие системы видеонаблюдения позволяет совершать визуальный контроль происходящего на объекте, его преимущества состоят в том что нет необходимости закреплять за каждым сервером персонального охранника, поскольку контролируется объект дистанционно и кроме того круглосуточно, а также есть возможность, при возникновении потребности, просмотреть запись видео с камер наблюдения с целью выявления нарушения.

Для всестороннего обеспечения безопасности для центра данных следует уделять внимание таким угрозам как – пожар, задымление и т.п, для устранения которых необходимо оперативно оповестить сотрудников предприятия и службу безопасности, одним из самих эффективных методов оповещении является автоматизированная система для пожаротушения, которая действует на очаг возгорания еще в процессе его зарождения и дает возможность избежать масштабного распространения огня и минимизировать ущерб.

Система контроля и администрирование доступа позволяет автоматизированным способом управлять входами-выходами, ограничивать доступ пользователей на определенной территории, вести статистику посетителей, наблюдать за перемещением по территории пользователей и т.д. Требуется отметить что подобные системы способны идентифицировать лица, цвета, автомобильные знаки и т.д., и исходя из полученной информации делать определенные выводы о одобрению или отказе в доступе к определенной зоне.

Таким образом, центр данных способствует построению многоуровневых систем для хранения данных, привлекая различные технологии для распределенных сетей хранения информации, ЦОД предоставляет возможность для защиты данных от физического и логического повреждения путем создания систем резервного копирования и репликации в них информации.

Системы резервного копирования и архивирования позволяют устранить влияние человеческого фактора на обеспечение хранения данных в облаке, а также оптимизировать процесс восстановления данных, которые важные для бизнеса.

Основными компонентами, которые необходимы для успешного построения системы информационной безопасности ЦОД, являются: централизованная система для руководства средствами защиты информации; средства которые помогают определить и предотвратить вторжения; средства антивирусной безопасности; средства для работы с шифрованием файлов; средства межсетевого экранирования; средства по ограничению доступа; средства по аналитике и руководству событиями; средства за проведением мониторинга по целостности информации и приложений.

Для эффективного обеспечения конфиденциальности и надежности использования облачных систем нужно, прежде всего, позаботиться о безопасности всех участников составляющих процесс передачи, хранения информации начиная от поставщика «облачного» решения, пользователя и других коммуникаций, которые их связывают. Если говорить о поставленных задачах перед провайдером, то они состоят в том, чтобы обеспечить неприкосновенность информационных данных третьими лицами, как в физическом, так и программном смысле. Для успешного решения подобных задач пользователь должен вести на пределах своей территории необходимую конфиденциальную политику данных, с целью исключения возможности по предоставлению прав доступа к данным посторонним лицам.

Если необходимо обеспечить целостность данных, когда используются через отдельные облачные приложения, то необходимо предпринять нужные действия, учитывая современный интерфейс баз данных, использовать системы, которые предназначены для резервного копирования, алгоритмы для проверки конфиденциальности данных и другие индустриальные решения, но кроме всего перечисленного, также, необходимо учитывать интеграцию нескольких «облачных» приложений от нескольких поставщиков.

Если сравнивать возможные риски, касающиеся безопасности данных в известных облачных моделях, и возможных альтернативных решений вопросов по безопасности, то в зависимости от модели SaaS,

PaaS или IaaS, изменяется уровень контроля над безопасностью и физическая интерпретация решения. Приведем наиболее актуальные угрозы для информационных баз на Рис. 1 [2-4].

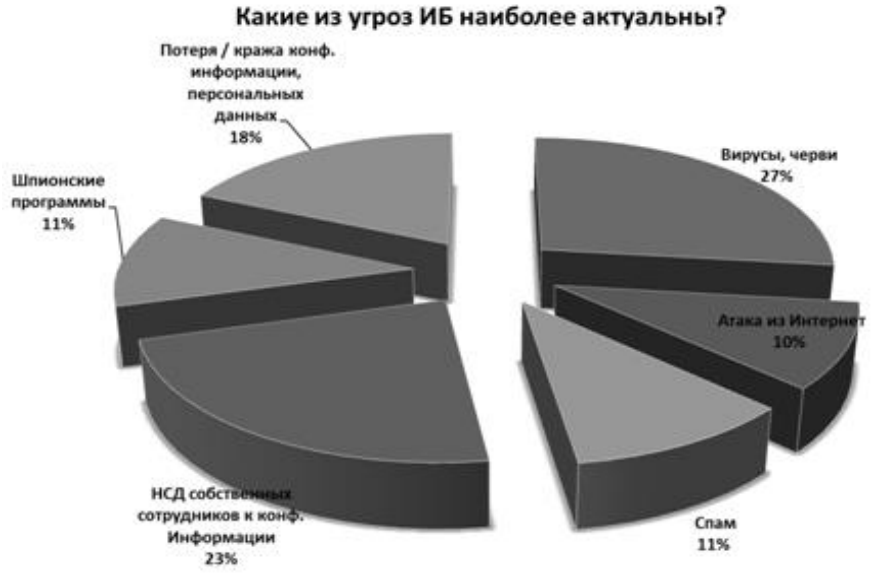

Рис. 1. Существующие угрозы для информационных баз

Рассмотрим по отдельности вопрос обеспечения безопасности в каждой из известных облачных систем. В модели SaaS приложение доступно через веб-браузер и запускается на облачной инфраструктуре, в этом случае клиент не имеет возможности управлять сетью, серверами, ОС, сбережениям информации и даже некоторыми дополнительными возможностями используемых приложений. Исходя из этого при использовании модели SaaS, главная ответственность по предоставлению и обеспечениюбезопасности возлагается только на поставщиков и в связи с этим пользователь не имеет возможности управлять паролями.

Главным риском в модели SaaS является, то что приложения расположенные в облаке и возможно использование разных учетных записей для того чтобы получить доступ к приложению. Компании могут решить описанную проблему путем проведения унификации учетных записей для облачныъ и локальных систем. Если пользователь в едином лице будет контролировать вход в приложение, то в свою очередь он получит доступ к рабочим станциям и облачным сервисам, данный подход способствует уменшению количества «подвисших» учетных записей, которые могут быть подверженные взлому после увольнения сотрудников.

Использование модели PaaS предвидит, что клиент самостоятельно создает приложение на необходимых ему языках программирования и инструментах, а потом разворачивают их на облачные технологии. Аналогично модели SaaS, клиенти PaaS лишены возможности управления и контроля за инфраструктурой облачных приложений – сети, сервера, ОС, системы хранения данных, но пользователь имеет возможность развертывать приложения. Используя модель PaaS, клиенты должны учитывать вопросы о безопасности приложений, управления API, речь идет о подтверждении входа в систему, авторизации, проведения проверки.

Главная проблема которая возникает при использовании PaaS – это шифрование данных, отметим, что модель PaaS сама по себе безопасно, но возникает риск связанный с малой производительностью системы. Возникновение описанной проблемы прежде всего связано с тем что при осуществлении обмена информацией между провайдерами PaaS необходимо пользоваться шифрованием, но для этого требуется соответственна мощьность процессора, кроме того, известно, что любое действие передачи информации пользователей необходимо осуществлять по зашифрованому каналу передачи данных [1].

В IaaS клиенты не могут управлять облачной инфраструктурой, но вместе с тем они имеют доступ до контроля над ОС, сбережением информации и развертывания приложений, в редких случаях, возможно ограничение при выборе различных компонентов сети. Отметим, что в рассмариваемой модели существует несколько вариантов для обеспечения самой по себе безопасности, без всесторонней защиты инфраструктуры, из этого следует то, что клиенты сами должны организовать безопасность используемой операционной системы, информационного контента, приложений, за счет API.

Выделим основные элементы, защиту которых должен предоставить провайдер: непосредственный контроль за доступом к инфраструктуре; устойчивость используемой архитектуры. Со стороны

пользователя должны быть защищены следующие объекты: межсетевой экранирование в пределах используемой инфраструктуры; защиту ОС, информационных баз(доступ, устойчивость, настройки безопасности); защиту финишных ланок приложений (антивирусная защита, контроль за входом в систему) [3].

Легко видеть, що значительно большая часть для успешной организации защиты облачных технологий ложиться на плечи клиентов, а что касается провайдера, то он скорее всего предоставляет стандартные рекомендации, которые необходимо выполнять для полноценной защиты данных, нежели решает поставленные задачи перед пользователями.

Для лучшего визуального понимания распределения ответствености, за организацию безопасности, между пользователем и поставщиком услуги приведем следующую таблицу 1 [2].

Таблица 1. Распределение обязаностей по обеспечению безопасности между клиентом и поставщиком услуги. (П - поставщик, К - клиент)

	Сервер предприятия	**IaaS**	**PaaS**	**SaaS**
Приложение	К	К	К	П
Данные	К	К	К	П
Реализация	К	К	П	П
Програмная среда	К	К	П	П
ОС	К	К	П	П
Виртуализация	К	П	П	П
Сервера	К	П	П	П
Хранилища информации	К	П	П	П
Оборудование сети	К	П	П	П

Проведенный анализ литературных источников по тематике данной статьи, показывает, что науке известно 7 основных направлений атак на сервисные модели SaaS, PaaS и IaaS, такие как:

1) нарушение конфинденцеальности при использовании облачных технологий;

2) нарушение безопасности при использовании програмных интерфейсов (API);

3) нарушение внутри компании пользователя;

4)нарушение целостности систем виртуализации;

5) нарушение правил аутентификации, авторизации и аудита, что влечет за собой потерю или утечку информации;

6) нарушения целостности персональных данных предоставляющих доступ к необходимым сервисам;

7) нарушения устойчивости внутренней инфраструктуры системы [1].

Результатом совместной работы организаций TCG и CSA, стосовно успешной организации безопасности облачных систем на всех ее этапах работы, стали сформированые рекомендации, которые должны быть учтены при заключении договора между клиентом и провайдером. Согласно рекомендациям специалистов необходимо: использовать технологии шифрования для предоставления сохранности данных; защитить данные при передачи, для этого нужно использовать надежные протоколы и алгоритмы (например TLS, IPsec и AES); организовать высокий степень аутенфикации; изолировать пользователей друг од друга в том плане, что данные и приложения одного клиента дожны быть отделены от других пользователей; провайдеру следовать единой стратегии в нормативно-правовом аспекте; разработать документальные подтверждения на незапланированные проишествия.

Выполнение предоставленных советов позволит решить множество вопросов, связанных с безопасным использованием облаков, предоставляет варианты для выхода из форс-мажорных обстоятельств, разъясняет, как себя вести при смене провайдера, предоставляющего облачные услуги, и успешное решение других вопросов в этом направлении.

Проведя детальное изучение вопроса по обеспечению безопасности работы при использовании облачных технологий, отметим перспективные тенденции развития в этом направлении. Для того чтобы надежно обеспечить безопасность сбережения информационных данных, необходимо будет на уровне каждой кампании создавать частную облачную систему, поскольку частные облака по сравнению с публичными и гибридными, имеют наиболее схожую виртуальную инфраструктуру, к слову, крупные отделы ИТ-компаний на сегодняшний день уже успешно реализовывают описанную идею на практике и в итоге имеют возможность полностью контролировать облачные приложения. Если говорить об обеспечении защиты информации в публичном облаке, то существует множество угроз для сохранения целостности информации, связанных с взломом системы.

Выводы.

В статье проведено исследование основных подходов для обеспечения защиты информации при использовании облачных систем. Проведен анализ научных достижений в данном направлении,

позволил более конкретизировать полученные, в настоящее время данные по поводу возможных угроз информационных баз, на основе которых приведен рис.1.

Мы видим, что использование облачных вычислений представляет собой значительный прогресс в сфере развития информационных технологий и сервисов. Пользователь имеет возможность в доступе к различным источникам вычислительных ресурсов. Следует отметить, что облачные вычисления имеют множество преимуществ в плане скорости обмена информацией, оперативности, эффективности, где главную роль играет безопасность проведения подобного вида действий.

Основные аспекты организации безопасности облачных вычислений были рассмотрены в рамках нашей статьи. В таблице 1. приведены данные по распределению ответственности, за организацию безопасности, между пользователем и поставщиком предоставляющих услуг. Следует помнить о том, что выбранные средства защиты должны напрямую зависеть от особенностей облачной технологии.

В связи с этим становится ясно, что идеальным решениям для того чтобы убедить клиента в том что его данные будут в безопасности является соответствие предоставленных облачных услуг требованиям документов и стандартам для того чтобы обеспечить безопасность информационных данных. Другим вариантом, предоставления безопасности облачных услуг является выбор способов защиты информации, поставщиками облачных услуг из уже известных на рынке готовых решений.

Принимая во внимание все возможны сложности использования облачных систем в плане безопасности защиты данных, облака имеют в разы большие преимущества используя сервисы Интернет и становятся все более популярными на современном рынке информационных технологий, что вызывает интерес для продолжения исследований в данном направлении.

Список литературы / References

1. *Mell Peter, Grance Thimothy.* «The NIST Definition of Cloud Computing (Draft)» // Recommendations of the National Institute of Standards and Technology, Special Publication 800 – 145 (Draft), Сентябрь, 2017.
2. «Автоматизация технологических объектов и процессов. Поиск молодых» / Сборник научных трудов XVII научно-технической конференции аспирантов и студентов в г. Донецке 24-25 мая 2017 г. Донецк: ДонНТУ, 2017.
3. *Бакст Л.А., Бурляева О.К., Кузнецова В.В., Малышева Е.В.* Реализация облачных вычислений – актуальная задача развития информационно-вычислительных сетей / Л.А. Бакст, О.К. Бурляева, В.В. Кузнецова, Е.В. Малышева // Профессиональные инновации. № 7. Москва, 2013. С. 26–36.
4. *Синев П.В.* Облачные вычисления: перспективы и проблемы / П.В. Синев // Материалы научно-практической конференфии студентов и аспирантов. г. Владимир, 2012. 2 с.
5. *Ширманов А.* Безопасность виртуализации при обработке данных ограниченного доступа // Москва, ЭКСПОЦЕНТР, InfoSecurity Russia. 30 сентября 2009.
6. *Шмойлов Д.В.* Облачные вычисления: актуальность и проблемы / Д.В. Шмойлов // «Электронное научное периодическое издание Электроника и информационные технологи». № 1 (10)». МГУ им. Н.П. Огарева, г. Саранск, 2016. 7 с.