Макаров Дмитрий Александрович
магистрант
ФГБОУ ВО «Армавирский государственный
педагогический университет»
г. Армавир, Краснодарский край
Коновалова Виктория Александровна
учитель обществознания
МАОУ – СОШ №7 им. Г.К. Жукова
г. Армавир, Краснодарский край

ОДИН ИЗ ПОДХОДОВ К ЗАЩИТЕ ИНФОРМАЦИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

***Аннотация**: в данной статье рассматривается вопрос о защите данных в облачной среде. На данный момент защита информации в облаке является серьезной проблемой в сфере информационных технологий.*

***Ключевые слова**: информация, облачная среда, шифрование.*

На сегодняшний день облачная среда развивается быстрыми темпами, и провайдеры активно пытаются убедить рынок информационных технологий, что облачные вычисления являются безопасным решением, как для рядовых пользователей, так и для госструктур и бизнеса.

Информация, которая хранится в облаках, может представлять, как общедоступную (музыка, фильмы и т. д.) так и конфиденциальную информацию. Соответственно при потере или утечки данных фирма может понести не только большие финансовые убытки, но и подорвать свою репутацию.

Серьезной угрозой при использовании облачной среды становится тот факт, что пользователь, удалив какие-либо данные из облака, не может быть полностью уверен в том, что информация удалена безвозвратно.

На сегодняшний день предоставить определенную гарантию контроля над данными и вычислениями может использование криптографических протоколов.

Однако полноценных решений, которые могут гарантировать защиту данных при обработке их в облаке нет.

Шифрование данных может происходить на разных уровнях. Рассмотрим структуру стандартного облачного приложения. Обычно в нее входит подсистема хранения, веб-сервера, сервера приложений, СУБД, сети и клиентского приложения. Рассмотрим, на каких уровнях возможно использование шифрования данных.

Шифрование канала должно происходить между облаком и клиентом, чтобы злоумышленник не мог вмешаться в процесс передачи данных и допустить утечку информации. Здесь концепция уже выработана – протоколы SSL с аппаратным ускорителем при синхронизации с облаком. Конечно, было более правильно SSL-шифрование организовать непосредственно в виртуальной машине, однако решения должны быть на уровне гипервизора.

Так как в облаке виртуальная машина является файлом с образом памяти и процессов, соответственно доступ к файлу дает злоумышленнику ценную информацию [1, с. 25]. Поэтому оптимальным вариантом было бы шифровать непосредственно виртуальные машины при передаче их между узлами и при хранении в неактивном состоянии. Но реализация этого механизма шифрования должен быть исполнен на уровне гипервизора, непосредственно самим производителем систем виртуализации. Пока подобных решений нет.

В данном случае шифруется отдельный виртуальный диск, который монтируется к виртуальной машине в облаке. Этот метод шифрования защищает от кражи данных с виртуального диска, к примеру, во время *BackUp*. Так же администраторы виртуальной инфраструктуры, имеют полный доступ и возможность манипулировать виртуальными машинами и их файлами (копирование и просмотр файлов виртуальных машин, получить доступ к хранилищу и т. д.), по сути, они являются, супер-пользователями, ошибки либо злонамеренные воздействия, которое смогут привести к угрозе информационной безопасности. Следо-

вательно, если злоумышленник получил доступ к виртуальной машине, к которой этот диск монтируется, то такой метод шифрование не сможет защитить данные [3, с. 115].

Если вы приняли решение хранить данные в «облаке», то должны понимать, что в данной ситуации ваши конфиденциальные данные должны шифроваться с момента возникновения (создания) и до самой «смерти». На сегодняшний день самая надёжная форма шифрования является криптография на клиенте, с последующей передачей в облако только набор бит. В данном случае вся обработка данных будет осуществляться на клиенте, следовательно, теряется все преимущества облачных технологий. Для этого стоит шифровать на клиенте только наиболее ценные данные, утечка которых приведёт к серьёзным потерям. В частности, ключи шифрования стоит хранить только на клиенте и передавать их в облачные приложения только при авторизации. Так же нужно оговорить процедуру гарантированного уничтожения этих ключей по истечению времени. Следовательно, лучше всего использовать схему шифрования, при которой используется временный ключ, который будет действительным на ограниченный интервал времени [2, с. 15].

Рассмотрен один из подходов по обеспечению информационной безопасности облачных вычислений, основанный на шифровании данных на различных уровнях. Поскольку, зашифровав только одну часть облака, не предоставляется возможность защитить конфиденциальную информацию полностью, поэтому для защиты данных на облачных сервисах нужен комплексный подход системы шифрования со своими специфичными протоколами. Для этого нужно тесное, а самое главное взаимовыгодное сотрудничество клиента и оператора облачного сервиса ведь система безопасности, которая позволяет сохранить тайну, будет привлекать новых пользователей ресурса, кому не безразлична конфиденциальность расположенных документов в облаке. Так же одно из главных звеньев являются производители программного обеспечения для облачных технологий и быстрая адаптация уже существующих продуктов для традиционных систем.

Список литературы

1. Джордж Риз Облачные вычисления. – СПб.: БХВ-Петербург, 2011.

2. Питер Фингар Dot.Cloud: облачные вычисления – бизнес-платформа XXI века. – М.: Аквамариновая Книга, 2011.

3. Сергей Панасенко Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009.

4. Сухарев Е.М. Информационная безопасность. Методы шифрования. – М.: Радиотехника, 2011.

5. Василий Леонов Google Docs, Windows Live и другие облачные технологии. – М.: Эксмо, 2012.

6. Сафонов В.О. Платформа облачных вычислений Microsoft Windows Azure. – М.: Бином; Лаборатория знаний, 2013.

7. [Электронный ресурс]. – Режим доступа: http://www.diplomy.su/shop/82.html (Сохраненная копия)