А. В. Царегородцев, М. М. Лавриненко, Н. В. Лапенкова

ОЦЕНКА РИСКА БЕЗОПАСНОСТИ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Введение

Достижение целей информационной безопасности (ИБ) организации становится одним из ключевых факторов для принятия решений об услугах аутсорсинга информационных технологий и, в частности, для принятия решения о миграции организационных данных, приложений и других ресурсов на инфраструктуру, основанную на среде облачных вычислений [1].

Провайдеры, предоставляющие общедоступные облачные сервисы, как правило, не имеют четкого представления о требованиях безопасности конкретной организации. В связи с этим организации должны иметь возможность использовать систему управления информационной безопасности (СУИБ) для облачных приложений и сервисов, соизмеримую или превосходящую ту, которая используется для систем, развернутых в рамках традиционной ИТ-модели.

Информационная безопасность облачной среды имеет прямую зависимость от индивидуальной безопасности каждого компонента архитектуры: сервиса, системы самообслуживания, системы управления квотами на ресурсы, гипервизора (программы управления операционными системами), системы управления гостевыми виртуальными машинами, промежуточного программного обеспечения и системы хранения данных.

Мониторинг, решение проблем и контроль безопасности являются критически важными процессами в организации наряду с производительностью и доступностью. В связи с тем, что облачные вычисления несут новые вызовы в области информационной безопасности, для организации крайне важно контролировать процесс управления информационной безопасностью облачной инфраструктуры. Уровень доверия к предоставляемым сервисам может значительно меняться в зависимости от целей организации, структуры ее активов, открытости для публики, угроз, которым подвергается организация, а также приемлемого уровня информационного риска [2].

1. Ключевые вопросы информационной безопасности облачных сред

Управление информационными рисками, определение пригодности облачных сервисов для организации невозможно без понимания контекста, в котором работает организация и последствий от возможных видов угроз, с которыми она может столкнуться в результате своей деятельности. То, что хорошо работает для одной организации, не обязательно будет работать для другой, большинство организаций не могут себе позволить в финансовом отношении защитить все свои вычислительные ресурсы и активы, поэтому особое внимание должно уделяться вариантам обеспечения безопасности на основании соотнесения стоимости решения, а также критичности обрабатываемых данных.

Анализ основных преимуществ использования облачных сред в качестве основы для построения информационно-телекоммуникационных сред показывает, что, несмотря на все преимущества, предоставляемые облачными решениями, такими как высокая масштабируемость, эластичность, учет потребления и самообслуживание по требованию, остаются нерешенными задачи обеспечения информационной безопасности таких систем.

Слабой стороной общедоступной среды облачных вычислений с точки зрения информационной безопасности является невозможность гибкого управления и контроля состояния информационной безопасности инфраструктуры со стороны клиента (организации). Приведем наиболее серьезные нерешенные задачи безопасности общедоступной облачной среды.

- Отсутствие контроля над состоянием аппаратной части. Контроль над состоянием виртуальной части облачной инфраструктуры могут осуществлять только IaaS-клиенты, в то время как PaaS- и SaaS-клиенты такой возможности не имеют.

- Отсутствие подробного журнала. Провайдеры общедоступных облачных сред не предоставляют возможности ведения детального журнала для анализа действий пользователей и администраторов системы, что может сильно усложнить расследование инцидентов информационной безопасности.

- Трудности с доступом к доказательной базе. Сохранение и выемка доказательной базы в случае незаконной деятельности клиента могут быть затруднены в силу географического распределения данных в рамках инфраструктуры провайдера.

- Отсутствие прозрачности работ провайдера. С точки зрения клиента общедоступного облака, набор предоставляемых услуг выглядит как черный ящик без исходного кода используемых приложений, что имеет целью обеспечить конфиденциальность некоторых аспектов защиты облачных сервисов и предотвратить использование «узких мест» инфраструктуры провайдера.

- Зависимость от канала связи. Для эффективного использования облачных сервисов требуется наличие широкополосного доступа в Интернет. Отсутствие требуемой пропускной способности сети может сильно снизить время реакции системы на действия конечного пользователя.

- Сложные процедуры миграции данных. Миграция данных (начальная загрузка) в публичную среду облачных вычислений или смена провайдера является серьезной проблемой и требует больших финансовых и людских затрат со стороны клиента.

Приведенные нерешенные задачи информационной безопасности не позволяют построить защищенные облачные сервисы для обработки критичных активов. Только включение в архитектуру демилитаризованных зон (ДМЗ) в виде частной облачной среды может позволить обеспечить требуемый уровень безопасности обрабатываемых данных.

2. Подходы к оценке риска

Управление информационными рисками является центральным процессом обеспечения информационной безопасности. Для каждого информационного актива нужно определить уровень его уязвимости, наличие потенциальных угроз, способных использовать эти уязвимости, а также оценить влияние инцидентов безопасности на бизнес-процессы организации в рамках повседневной работы. Поставщики облачных технологий используют различные механизмы для обеспечения безопасности. Однако существуют два основных вопроса, связанных с обеспечением информационной безопасности организации [2]:

1) как оценить риск для безопасности данных, прежде чем приступить к работе в облаке?

2) как убедить клиентов, что их данные и программы в безопасности в центре обработки данных (ЦОД) облачного провайдера?

Если пользователь облачного сервиса способен оценить риск безопасности данных, то он может определить уровень доверия к поставщику услуг. Если риск безопасности данных высокий, то это приводит к снижению доверия.

Пользователю услуг необходимо иметь четкое представление о методах, принятых поставщиками услуг для обеспечения безопасности информации. Современные технологии обеспечения безопасности дают возможность создания определенного уровня доверия в сфере облачных вычислений. Например, SSL (протокол Secure Socket Layer), цифровые подписи и аутентификация протоколов для доказательства методов аутентификации и контроля доступа при управлении авторизацией. Однако сами методы не могут дать методику определения достоверности. SSL, например, не может сам по себе доказать, что сообщение между сервером

и несколькими хостами является безопасным. Кроме того, есть вероятность нескольких точек отказов в облачной среде.

Современные технологии безопасности не обладают эффективными инструментами для определения достоверности информации. Анализ отечественных и зарубежных публикаций показал, что большинство авторов согласны с таким определением понятия «доверие»: «Доверие является определенным уровнем субъективного представления о вероятности, с которой агент будет выполнять определенное действие, в то время как мы можем контролировать такие действия, и в контексте, в котором он касается наших собственных действий» [2]. Исходя из этого определения можно сказать, что доверие является субъективной оценкой и зависит от тех действий, которые мы не можем контролировать.

Можно выделить три вида моделей доверия в распределенных системах:

1) прямое (полное) доверие;

2) доверительные отношения;

3) допустимое доверие.

В облачных технологиях, в которых данные и программы, по сути, являются трансграничными, доверительные отношения могут иметь решающее значение для определенного типа приложений. Модель прямого доверия существует в облаке, когда есть общая сущность доверия, когда выполняются все заявленные аутентификации и генерации учетных данных, которые связаны с конкретными лицами.

Ключевая разница с другими моделями в том, что прямая модель доверия не позволяет делегировать заявленные аутентификации. И каждая проверяющая сторона должна использовать эту структуру. Примером такого типа доверия является использование PKI (Инфраструктура Публичного Ключа), где проверка подлинности на основе ключевых центров сертификации (ЦС) дает все виды доверительных отношений. Ответственность за безопасную передачу данных лежит на сертифицирующих органах (удостоверяющих центрах).

3. Оценка риска в облачных вычислениях. Использование матрицы доверия

Очень сложно найти подходящую единицу измерения для определения доверия, но есть несколько производных переменных (например, данные о затратах), которые могут быть использованы для его описания. На основании значимых факторов безопасности строится матрица доверия и проводится анализ рисков безопасности данных. При построении матрицы доверия некоторые эвристики могут быть использованы для выбора параметров безопасности.

В облачной среде стоимость данных, как правило, зависит от оценки пользователей, основанной на критичности данных. Существует большое многообразие факторов, влияющих на критичность данных. Так, например, конфиденциальная коммерческая информация может быть важной, и поэтому ей назначается более высокая стоимость по сравнению с менее критическими данными.

Кроме того, история провайдера может являться допустимым параметром для оценки риска. История включает в себя профиль провайдера, его «заслуги» в прошлом. Если пользователи не удовлетворены качеством конкретного сервиса, предоставляемого провайдером, это существенно повлияет на фактор доверия. Если поставщик услуг не обладает хорошей историей безопасности данных (например, если последняя запись является записью о нарушении безопасности), то она может также уменьшить фактор доверия. При этом и другие переменные также могут быть использованы для создания матрицы доверия, например поддержка шифрования, стоимость услуги, поддержка мониторинга и т. д.

Наряду с матрицей доверия существует ряд параметров, также используемых для измерения доверия и позволяющих точно настроить доверительные переменные. Параметры, которые мы выбираем в этой категории, — это расположение данных, соблюдение установленных норм.

Вышеперечисленные параметры необходимы в качестве механизма поддержки в матрице доверия. Они используются для проверки факторов, которые обеспечивают поддержку принятия решения при анализе рисков.

Используя матрицу доверия, где оси отражают используемые переменные, свяжем их по значению друг с другом. Рис. 1 дает графическую интерпретацию матрицы доверия для анализа риска, где низкий риск — зона высокого доверия, а высокий риск — зона низкого доверия.

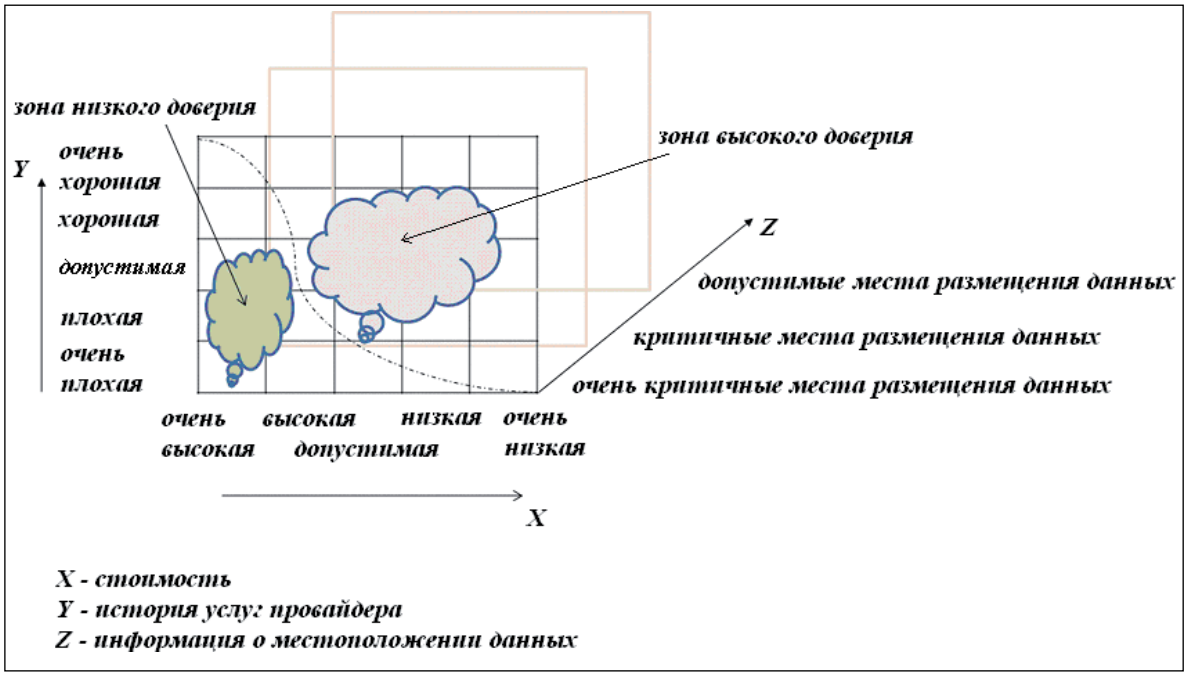

Рис. 1. Матрица доверия для анализа степени риска

Тогда очевидно, что высокая стоимость данных наряду с плохой историей поставщика услуг и в сочетании с очень критичными местами размещения данных приведет к более высокому риску — меньшему доверию.

Зона высокого доверия может указать риск безопасности для текущих операций, а также для будущих сделок с этим сервисом провайдера. Такой превентивный подход к оценке риска рассматривается как часть профилактической или реактивной меры. Например, добавленный уровень аутентификации и/или проверки пользователя может быть использован для процессов, которые связаны с зоной низкого доверия. Этот метод может быть использован для оценки доверия и для осуществления последующих операций с данными. На основе этого метода можно определить доверительные действия для всех будущих сделок с поставщиком облачных услуг.

Согласно данным, приведенным IDC (International Data Corporation), пока для обеспечения целостности и непротиворечивости данных, хранимых в облаках, используются только криптографические средства защиты. В техническом описании на AWS (Amazon Web Services) рассматриваются физическая безопасность, резервное копирование и использование соответствующих сертификатов [3]. Аналогичным образом, другие поставщики, такие как Google, Microsoft и т. д., рассматривают альтернативные механизмы обеспечения безопасности в облаке [4, 5].

В работе [6] проводится анализ тех семи значимых рисков, которые клиент должен оценить, чтобы использовать инфраструктуру облачных вычислений. В дополнение к этим семи рискам мы также определили ряд других определяющих факторов, которые должны учитываться при выборе провайдера облачных сервисов. Эти вопросы включают хранение данных, безопасность сервера,

привилегированный доступ пользователей, виртуализацию и переносимость данных. Для принятия риска безопасности данных предлагается определить ключевой набор переменных доверия, в результате чего возможно построение доверительной матрицы, основанной на безопасности данных в облачных вычислениях.

Заключение

Изменение контура безопасности, выход критичных активов организаций из-под внутреннего контроля с последующей миграцией этих активов в облачную среду определили основную цель настоящего исследования, которая заключается в совершенствовании методов управления информационной безопасностью информационно-телекоммуникационных сред, функционирующих на основе технологии облачных вычислений. В работе представлен один из подходов к анализу рисков безопасности данных в облачных средах.

Предложенный подход, с одной стороны, поможет провайдерам облачных услуг обеспечивать своих клиентов сервисами, удовлетворяющими критериям безопасности данных. С другой стороны, этот подход может быть использован пользователями облачных сервисов для оценки риска и принятия решения о миграции критичных данных в облачную инфраструктуру.

В настоящее время отсутствует системный подход к анализу рисков в средах облачных вычислений. Предложенный подход легко адаптируется для автоматизации процесса анализа рисков в корпоративных сетях организаций, функционирующих на основе технологии облачных вычислений.

СПИСОК ЛИТЕРАТУРЫ:

1. *Царегородцев А. В., Качко А. К.* Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность. 2012. № 1 (18). С. 46–59.
2. *Царегородцев А. В.* Анализ рисков безопасности данных в корпоративных сетях кредитно-финансовых организаций на основе облачных вычислений // Национальные интересы: приоритеты и безопасность. 2013. № 39 (228). С. 35–44.
3. Overview of Security Processes (2011).
4. URL: http://appengine.google.com (дата обращения: 12.12.2013).
5. URL: http://www.mesh.com (дата обращения: 12.12.2013).
6. *Brodkin J.* Seven Cloud Computing Security Risks (2008). URL: http://www.gartner.com/DisplayDocument?id=685308 (дата обращения: 12.12.2013).