ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОЦЕССОВ ОБРАБОТКИ ДАННЫХ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Царегородцев Анатолий Валерьевич
Доктор технических наук, профессор,
Всероссийская государственная налоговая академия
Министерства финансов Российской Федерации (Москва)
05.13.19
academic_tsar@mail.ru

Аннотация. *Широкое распространение и применение облачных вычислений диктует необходимость адаптации и доработки существующих моделей безопасности компьютерных систем. Для достижения конфиденциальности данных на основе существующих моделей развёртывания облачных сервисов предлагается процедура распределения рабочего процесса между компонентами среды облачных вычислений.*

Ключевые слова: облачные вычисления, публичное облако, частное облако, гибридное облако, требования безопасности, теория графов, конфиденциальность данных.

SECURITY OF DATA PROCESSING IN THE CLOUD COMPUTING

Tsaregorodtsev Anatolii Valerievich
Doctor of Technical Sciences, Professor,
The State Tax Academy of Russian Federation (Moscow)

Abstract. *Use of cloud computing applications and services requires review and adaptation of existing formal models for computer security. It is necessary to consider the benefits of cloud deployment models and provide the procedure for allocating process among components of cloud computing environment for achieving confidentiality and data protection.*

Key words: cloud computing, public cloud, private cloud, hybrid cloud, security requirements, theory of graphs, data confidentiality.

Введение

Облачные вычисления в ближайшем будущем станут одной из самых распространенных ИТ технологий для развертывания приложений, благодаря своим ключевым особенностям: гибкости решения, доступности по запросу и хорошим соотношением цена/качество.

Под облачными вычислениями будем понимать модель, позволяющую осуществлять повсеместный и удобный доступ по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, совокупность сетей, серверов, хранилищ данных, приложений и услуг), который может быть оперативно предоставлен сервисным провайдером [1].

Необходимо отметить, что самыми критичными вопросами при построении инфраструктуры, основанной на среде облачных вычислений, являются аспекты обеспечения информационной безопасности. Достижение целей информационной безопасности организации, является ключевым фактором для принятия решений об услугах аутсорсинга информационных технологий и, в частности, для принятия решения о миграции информационных активов организации на различные модели предоставления облачных сервисов. Большинство организаций не могут себе позволить защитить все свои вычислительные ресурсы и активы в силу бюджетных ограничений, поэтому при переходе на новую модель предоставления ИТ-услуг особое внимание

должно уделяться вопросам обеспечения безопасности обработки информации.

1. Общие требования информационной безопасности облачных вычислений

Рассмотрим ряд факторов, которые должны всегда рассматриваться в качестве основы построения облачной конфигурации.

Затраты и ресурсы. С одной стороны финансовые ресурсы облачного провайдера ограничивают его в инвестициях на усовершенствование технологий управления информационной безопасностью. Отсутствие неограниченных ресурсов может мотивировать провайдера серьёзно подойти к вопросам проектирования, построения архитектуры и решения. С другой стороны уменьшение стоимости ИТ решения – это главная мотивация для потребителя облачных услуг. Природа этих ограничений приводит к развитию сервисов с рабочими характеристиками, которые не идеальны для всех потребителей.

Надёжность. Под надёжностью понимается свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования [2].

Производительность. Совокупность нескольких свойств, которые имеют отношение к полезности системы. К примеру, общие меры включают оперативность реагирования на входную информацию (чувствительность) и пропускную способность системы при обработке.

Целостность. Конфиденциальность. Доступность. Это основные принципы информационной безопасности для всех типов систем, главная цель при построении комплексной защиты это соотнесение этих показателей с надежностью, производительностью и стоимостью решения.

Правовые и нормативные ограничения. Нормативно-правовые ограничения могут привести к необходимости учета дополнительных требований, связанных с техническими контролями безопасности, политики доступа, хранения данных.

Рассмотрим требования безопасности, которые выдвигаются для *физической безопасности* облачного центра обработки данных. Физическая безопасность объекта должна включать системы защиты с отдельными элементами безопасности, обеспечивающей многоуровневую защиту. Эти элементы включают в себя аспекты:

- природоохранного проектирования,
- контроля доступа (в том числе механического, электронного и процедурного),
- мониторинг (в том числе видео-, тепловой, близость наряду с экологическими датчиками),
- идентификации персонала и управления доступом,
- обнаружения вторжений с оповещением.

Физическая безопасность на объекте должны быть многоуровневой, каждый элемент должен быть интегрирован в общий автоматизированный центр контроля и управления.

Наряду с уникальными требованиями к безопасности облачной архитектуры, существуют общие, которые должны отвечать требованиям соответствующих стандартов, например, ISO 27001 и ISO 27002, так как они содержат практическую ценность, опыт, отчёты и рекомендации лучших практик.

Кроме того, все аспекты безопасности должны быть отражены в документе **«Политика информационной безопасности организации»** («Политика облачной безопасности»), которая имеет статус официального документа, согласовывается и утверждается высшим руководством. Политика безопасности должна рассматриваться, как фундамент построения всей системы, и не должна содержать подробных технических или архитектурных подходов (так как они могут меняться чаще, чем сама политика). Основная цель политики должны заключаться в определении основополагающих организационных и управленческих решений в области построения комплексной безопасности облака. Например, политика должна

объяснить необходимость применения шифрования с помощью использования какого-либо коммерческого продукта, а не включать в себя техническое описание безопасности транспортного уровня, уровня, протоколы защиты информации или другие специальные средства.

Политика безопасности также должна иметь ссылки на следующие разделы [3]:

- Ряд руководящих принципов для обеспечения безопасности при разработке программного обеспечения, в процессах управления ИТ инфраструктурой, и других операционных процедурах.
- Политика допустимого использования ресурсов для каждой категории пользователя: от внутренних операций, выполняемых администратором до действий конечных пользователей. Этот раздел должен идентифицировать категории использования ресурсов, определить критичную информацию, доступ к которой запрещен, обозначить последствия для нарушений.
- Ряд стандартов безопасности для всех аспектов облачной архитектуры, от миграции данных до операционной деятельности.

Стандарты безопасности для облачных вычислений должны включать в себя:

1. **Средства управления доступом**. Детализация целей данного уровня должна быть достаточной для осуществления контроля физического доступа к ЦОД и логического доступа к системам и приложениям.
2. **Управление реагированием на инциденты безопасности**. Должно быть подробно описано назначение всех ролей и обязанностей различных сторон, наряду с процедурами и сроками обнаружения инцидентов.
3. **Резервное копирование системной и сетевой конфигурации.** Необходимо иметь гарантированно надёжную копию всех конфигураций, включая компоненты инфраструктуры, серверы, и другое сетевое оборудование для всех хост-систем.
4. **Тестирование безопасности**. Облачный провайдер должен выполнять и документировать результаты первоначального и периодического тестирования безопасности. Этот стандарт должен включать роли и обязанности, а также подробное описание, когда планируется проведение сторонних тестирований или аудита.
5. **Шифрование данных и связи.** Должны быть идентифицированы все функциональные области (например, веб-трафик сервера), утверждены криптографические алгоритмы и необходимая длина ключа шифрования.
6. **Политика строгих паролей.** Должны быть описаны ключевые аспекты при задании паролей (в частности, длина и состав) и как облачный провайдер будет проводить процедуру аутентификации.
7. **Непрерывный мониторинг**. Должно быть детально описано, как выполняется управление конфигурациями и изменениями (развитие и обновление) с целью поддержки требуемого уровня безопасности и сохранение ключевого требования к информационной безопасности – непрерывности бизнеса.

Существует ряд других областей безопасности, которые непосредственно управляются со стороны облачного провайдера:

1) прекращение неактивных сессий;

2) определение ролей и ответственностей для персонала, обслуживающего облако;

3) разделение обязанностей и матрицы полномочий;

4) управление магнитными и электронными средствами удаления информации;

5) управление удалением или использованием оборудования;

6) своевременное удаление пользовательских привилегий;

7) аварийное восстановление и обеспечение непрерывности операций.

2. Специфические требования к построению защиты облачных вычислений

1) ***Управление идентичностью***

Идентичность – основной элемент оперативной безопасности облака. Информация должна быть корректной и доступной для всех компонентов облачных вычислений, у которых есть утвержденная потребность в доступе. Требования включают в себя следующие цели:

1. Должны быть реализованы контроли для защиты конфиденциальности, целостности и доступности информации, подтверждающей идентичность.

2. Должна быть внедрена система управления идентичностью, которая будет поддерживать потребности для аутентификации облачных клиентов и привилегированных пользователей.

3. Должен быть использован принцип «федеративной идентификации», чтобы обеспечить мобильность для пользователя и представить единый механизм для внутреннего доступа [4].

4. Проверка идентичности пользователей во время регистрации в соответствии с политикой безопасности и юридическими требованиями.

5. Должно обеспечиваться сохранение исторической информации после удаления идентификатора пользователя для дальнейших правовых исследований

6. Необходимо при процедуре повторного назначения профиля полномочий от одного пользователя к другому убедиться, что не предоставляется доступ к предыдущим данным старого пользователя, его контексту, или другой частной информации.

7. Должны быть реализованы специальные средства для клиентов для проверки утверждения идентичности персоналом облачного провайдера.

2) ***Управление доступом***

Контроль доступа использует идентификационную информацию для обеспечения и ограничения доступа к операционной среде облака и поддерживающей её инфраструктуры. Требования включают следующие цели:

1. Обслуживающий персонал облака должен иметь ограниченный доступ к данным клиента. Персоналу может потребоваться доступ к гипервизору или к устройствам хранения данных, к хосту клиента виртуальных машин или непосредственно к данным клиента, но такой доступ должен быть жестко ограничен конкретными операциями, которые должны быть определены в политике безопасности и в сервисном соглашении об обслуживании (SLA).

2. Должна быть реализована многофакторная аутентификации для высоко привилегированных и критичных операций путём применения дополнительных элементов защиты.

3. Не допускается использование ролей со всеми полномочиями, даже для администратора должен быть настроен профиль, в котором не предусмотрена возможность получения доступа ко всем компонентам облака.

4. При назначении прав доступа должны быть заложены основные минимальные привилегии (LPP) и реализована модель ролевого управления доступом (RBAC) для ограничения доступа авторизованных пользователей на основе их роли [4].

5. Для всех удалённых доступов должен использоваться белый список IP адресов отправителей. Если это сделать невозможно, то необходимо реализовать доступ с помощью дополнительных механизмов, таких как шлюзы.

3) ***Управление ключами шифрования***

В облаке, шифрование в первую очередь рассматривается, как основной механизм для защиты данных в состоянии покоя (при хранении), а также между хранением и фазой обработки. Требования к управлению ключами включают в себя следующие задачи [5]:

1. Необходимо убедиться, что существуют меры контроля для ограничения доступа к данным о ключах шифрования.

2. Необходимо убедиться, что корневой каталог и подписка ключей осуществляется надлежащим образом.

3. Необходимо убедиться, что отмена действия ключа осуществляется без побочных эффектов или неоправданной задержки для нескольких сайтов инфраструктуры облака.

4. Необходимо убедиться, что существует процедура восстановления взломанных ключей, и она эффективно работает.

5. Необходимо обеспечить защиту и шифрование всех клиентских данных и образов виртуальных машин на всех этапах жизненного цикла.

*4) **Аудит системы и сети***

Журнализация событий информационной безопасности является залогом её успешного управления. В облаке, фиксация событий аудита будет происходить в принципиально разных зонах доверия. Таким образом, события безопасности должны быть признаны, как имеющие разную степень целостности данных. Ниже перечислены основные требования к проведению аудита событий:

1. Аудит является обязательным для всех операционных систем, от инфраструктуры и сетевых компонентов до клиентских виртуальных машин. Соглашение о конфиденциальности, а также контракты на обслуживание могут установить границы для того, как данные могут быть собраны виртуальной машине арендатора и его виртуальной сети.

2. Все связанные с безопасностью события должны быть записаны со всей исчерпывающей информацией, необходимой для анализа, включая правильное время, рассматриваемую систему, идентификаторы пользователей, соответствующие коды событий.

3. Правильная работа системы аудита и регистрации должна постоянно проверяться на основе периодический сигналов и системы «запрос-ответ».

4. Все журналы аудита должны постоянно и централизованно собираться в целях обеспечения их целостности и для поддержки своевременных предупреждений и мониторинга.

5. Все журналы аудита должны надежно храниться в течение времени, определенного в требованиях политики безопасности, желательно до бесконечности и поддерживать возможность долгосрочного анализа.

6. В случае необходимости для поддержки проверки юридических или оперативных потребностей арендаторов или клиентов, записи аудита будут продезинфицировать, чтобы поделиться с арендаторов и покупателей либо как часть службы безопасности или по мере необходимости.

7. Контроли должны быть реализованы для защиты конфиденциальности, целостности и доступности событий аудита, сбора протоколов аудита, логов хранения, обработки и отчетности.

*5) **Мониторинг безопасности***

Мониторинг безопасности основывается на журналы аудита, мониторинг безопасности сети (с использованием контроля трафика), и данных об окружающей обстановке (физическая безопасность). К требованиям мониторинга безопасности относят следующие:

1. Мониторинг безопасности должен запускаться, как ключевой сервис, доступный для удаленного управления в безопасном режиме.

2. Должно быть предусмотрено оповещение на основе автоматического распознавания критического события или инцидента безопасности.

3. Должна быть реализована доставка критических оповещений через различные средства для оперативного реагирования.

4. Средства для обеспечения безопасности персонала для расследования и уголовного преследования разворачивается инцидент или просто просмотреть журналы для улучшения механизмов оповещения или вручную идентифицировать случаи нарушения безопасности.

5. Должна быть обеспечена возможность обнаружения аномалий в облачной среде в виде сервиса для клиентов и пользователей.

6. Должны быть предоставлены функциональные возможности, позволяющие клиентам обнаружить вторжение или другие аномалии для моделей PaaS (платформы-как-услуга) и IaaS (инфраструктура как услуга) с целью

передачи кодов событий и оповещения облачного провайдера [5].

7. Мониторинг безопасности должен быть надежно осуществлен даже в условиях сбоя при генерации события и создания на его основе отчетности.

6) ***Управление инцидентами***

Управление инцидентами и реагированием на них должно быть зафиксировано в виде положений при составлении соглашения об уровне обслуживания и политики безопасности:

1. Должен быть построен формальный процесс для обнаружения, выявления, оценки и реагирования на инциденты на периодической основе.

2. Процесс управления инцидентами должен включать в себя составление периодических отчётов.

7) ***Тестирование и управление восстановлением***

Тестирование функций безопасности должно быть выполнено для всего программного обеспечения до его внедрения. Важно найти уязвимость и возможность проникновения при постоянном тестировании программно-аппаратного обеспечения облака. Для большей эффективности, тестирование должно проводиться совместно с системами мониторинга и управления конфигурацией для предотвращения ложных тревог и реагирования на инциденты. Конкретные требования включают в себя следующее [5]:

1. Должны использоваться отдельные среды для разработки, тестирования, переносе и продуктивного запуска для всех программных приложений и систем облака, включая развертывание патчей в продуктивной среде.

2. Процедуры управления исправлениями должны быть определены для всех компонентов инфраструктуры, серверов, систем хранения, программного обеспечения для виртуализации, приложений и компонентов безопасности.

3. Должна быть определена комплексная стратегия восстановления и формирования контрмер, которые можно было бы использовать для целого ряда обстоятельств: от ответа на известные угрозы до внедрения менее критических патчей для повышения безопасности и надежности работы облака.

8) ***Сетевое и системное управление***

Сетевое и системное управление должно быть реализовано для инфраструктур, осуществляющих хостинг клиентских данных, прикладных программ и всего сетевое оборудования, включая в себя все физические и виртуальные компоненты или услуги. Конкретные требования включают в себя следующее:

1. Должна быть обеспечена соответствующая изоляция, конфигурация и безопасность для всех облачных компонентов.

2. Должна быть реализована изоляция на уровне сети между различными функциональными областями облачной инфраструктуры начиная от создания разных сетей, включая физическое разделение и виртуализацию сети для общественно доступных компонентов (хостов виртуальных машин хостов и интерфейсов хранилищ данных в общественном облаке) до управления компонентами инфраструктуры

и обеспечения безопасности и сетевого администрирования. Усилить эти действия можно за счёт использования программных брандмауэров на виртуальных машинах [4].

3. Должно быть предусмотрено отделение аппаратной платформы от операционной системы (ОС) (или виртуальной машины) с целью запрета пользовательского доступа к аппаратной части из публичного доступа. Обратный доступ (из виртуальной машины к платформе) также должен быть предотвращен.

4. Должны быть применены контроли для усиления изоляции между виртуальными машинами, принадлежащими к различным клиентам.

5. Должен осуществляться контроль за целостностью:

- ОС,
- образов виртуальных машин,
- приложений инфраструктуры,
- сетевой конфигурации,
- программного обеспечения и данных клиента.

6. Должны применяться современные средства сканирования на предмет наличия вредоносных сигнатур.

3. Модель безопасности процесса обработки данных

Для определения модели безопасности рабочих процессов в среде облачных вычислений предлагается модифицировать классическую модель безопасности Белла-ЛаПадула за счёт добавления новых условий и компонентов с использованием ключевых элементов теории графов.

Процесс обработки данных рассмотрим в виде ориентированного графа, облачные сервисы и данные которого будут изображены в виде вершин. На рисунке 1 изображен граф, с помощью которого описано последовательное выполнение двух облачных сервисов с использованием нескольких элементов данных [5].

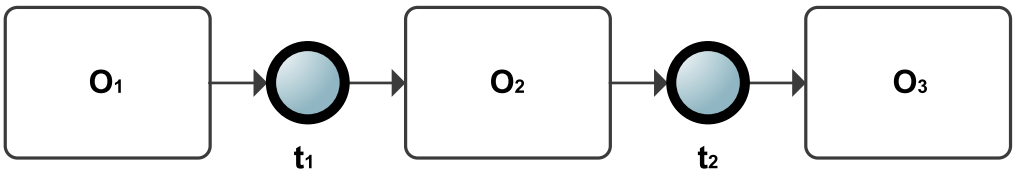

Рис. 1. Граф рабочего процесса с последовательным выполнением двух облачных сервисов.

Для формального описания требований безопасности воспользуемся положениями классической модели управления доступом Белла-ЛаПадула и рассмотрим два базовых свойства безопасности, которыми должен обладать каждый безопасный доступ субъекта к объекту [4].

- Доступ (*s,o,r*) обладает *ss-свойством* относительно $f = (f_s, f_o, f_c)$, где f_s – функция уровней доступа субъектов, f_o – функция уровней конфиденциальности объектов, f_c – функция текущих уровней доступа субъектов, когда выполняется условие:

$$r \in \{read; write\} \text{ и } f_s(s) \geq f_o(o).$$

- Доступ (*s,o,r*) обладает **-свойством* относительно $f = (f_s, f_o, f_c)$, когда выполняется одно из условий:

$$r = execute;$$

$$r \in \{read; write\} \text{ и } f_c(s) \geq f_o(o)$$

$$r = read; \text{ и } f_c(s) = f_o(o).$$

Основываясь на приведённых основных положениях классической модели безопасности, интерпретируем её по отношению к рабочему процессу, протекающему в среде облачных вычислений и выполняющему обработку над данными разного уровня конфиденциальности.

1. Представим облачные сервисы в виде субъектов (*T*), а данные в виде объектов (*O*).

2. Обозначим набор действий (*A*), который субъект (*T*) может совершить с объектами (*O*). В рамках данной задачи рассмотрим только действия чтения и записи.

3. Определим решетку безопасности (*L*) в виде таблицы, где для каждого блока процесса обработки данных обозначим требуемый уровень безопасности.

Блок процесса обработки данных	Уровень безопасности (*l*)	
o_1	1	Высокий
t_1	0	Низкий
o_2	0	Низкий
t_2	0	Низкий
o_3	0	Низкий
c_o	0	Низкий
c_1	1	Высокий

4. Определим матрицу текущих доступов для облачных сервисов, как $M : T \times O \to A$.

Сервис	Операция	Данные
t_1	Чтение	o_1
	Запись	o_2
t_2	Чтение	o_2
	Запись	o_3

5. Определим уровни конфиденциальности данных, как $B: S \times O \to A$.

Критичные данные o_1 должны храниться и обрабатываться только на частном облаке c_1, а данные o_2,o_3 можно хранить и в рамках общедоступного облака c_o.

Данные	Уровень конфиденциальности
o_1	1
o_2,o_3	0

6. Определим текущие уровни доступа сервиса к данным, как $C: S \to L$.

Сервис	Уровень доступа
t_1	1
t_2	0

7. Введём в модель новый элемент: карту текущих размещений блоков рабочего процесса $l: S + O \to L$.

Вершина графа	Частное облако c_1	Общедоступное облако c_o
o_1	x	
t_1	x	x
o_2	x	x
t_2	x	x
o_3	x	x

Модель Белла-ЛаПадула утверждает, что система безопасна, если для $\forall t \in T$ и $\forall o \in O$, выполняются условия: $B_{ui} \subseteq M_{ui}$ (1), $l(t) \le c(t)$ (2).

Запрет считывания информации сервисом, имеющим уровень доступа ниже уровня секретности информации, опишем как: $r \in B_{ui} \Rightarrow c(u) \ge l(i)$ (3). Запрет понижать уровень секретности информации, к которой обращается сервис, опишем как: $w \in B_{ui} \Rightarrow l(u) \le l(i)$ (4) [2].

Для адаптации классической модели безопасности к условиям среды облачных вычислений предлагается ввести новые переменные.

1. Карта размещений процессов обработки данных (P), которая будет включать в себя доступные компоненты среды облачных вычислений. Для рассматриваемого примера карта размещений состоит из двух компонентов:

Компонент	Уровень секретности
Частное облако c_1	1
Общедоступное облако c_o	0

2. Карта присвоений сервисов и данных к компоненту облака (H), которая будет использоваться для описания присвоения каждого сервиса и данных в облаке. Например, вариант присвоения $o_1^1 \to t_1^0 \to o_2^0 \to t_2^0 \to o_3^0$ означает, что данные o_1 размещаются в рамках частного облака c_1, а сервисы t_1, t_2 и данные o_2, o_3 размещаются в рамках общедоступного облака c_o.

Таким образом, можно сформулировать правило, позволяющее развернуть блок рабочего процесса (сервис или данные) на компоненте только в том случае, если уровень конфиденциальности компонента больше или равен текущего уровня доступа сервиса и уровня конфиденциальности данных. Если карта присвоений сервисов и данных к компоненту облака требует, чтобы данные o_1 располагались на облаке p_a, сервис t_1 на облаке p_b, данные o_2 на облаке p_c, то тогда должны выполняться условия: $l(p_a) \ge l(o_1)$, $l(p_b) \ge l(t_1)$, $l(p_c) \ge l(o_2)$ и $l(p_c) \ge l(o_2) \ge l(t_1)$.

4. Процедура распределения рабочего процесса между компонентами среды облачных вычислений

Используя полученную модификацию модели доступа Белла-ЛаПадула можно получить все варианты распределения рабочего процесса обработки данных в рамках среды облачных вычислений (V), где $V : T + O \to P$ [3]. Тогда полный набор возможных вариантов развёртывания рабочего процесса будет состоять из 16 различных комбинаций, где верхний индекс – это компонент, на котором развернуты данные или сервис.

Таблица 1

Множество возможных размещений блоков рабочего процесса между компонентами среды облачных вычислений

№	Вариант
1	$o_1^1 \to t_1^0 \to o_2^0 \to t_2^0 \to o_3^0$
2	$o_1^1 \to t_1^0 \to o_2^0 \to t_2^0 \to o_3^1$
3	$o_1^1 \to t_1^0 \to o_2^1 \to t_2^0 \to o_3^0$
4	$o_1^1 \to t_1^0 \to o_2^1 \to t_2^0 \to o_3^1$
5	$o_1^1 \to t_1^0 \to o_2^0 \to t_2^1 \to o_3^0$
6	$o_1^1 \to t_1^0 \to o_2^0 \to t_2^1 \to o_3^1$
7	$o_1^1 \to t_1^0 \to o_2^0 \to t_2^1 \to o_3^0$
8	$o_1^1 \to t_1^0 \to o_2^1 \to t_2^1 \to o_3^1$
9	$o_1^1 \to t_1^1 \to o_2^0 \to t_2^0 \to o_3^0$
10	$o_1^1 \to t_1^1 \to o_2^0 \to t_2^0 \to o_3^1$
11	$o_1^1 \to t_1^1 \to o_2^1 \to t_2^0 \to o_3^0$
12	$o_1^1 \to t_1^1 \to o_2^1 \to t_2^0 \to o_3^1$
13	$o_1^1 \to t_1^1 \to o_2^0 \to t_2^1 \to o_3^0$
14	$o_1^1 \to t_1^1 \to o_2^0 \to t_2^1 \to o_3^1$
15	$o_1^1 \to t_1^1 \to o_2^1 \to t_2^1 \to o_3^0$
16	$o_1^1 \to t_1^1 \to o_2^1 \to t_2^1 \to o_3^1$

Для осуществления перехода между двумя компонентами облачной среды предлагается ввести особый вид *транспортного сервиса*, который позволил бы преодолеть следующие ограничения:

1) сервис может генерировать выходные данные на другом компоненте облачной среды без необходимости предварительного сохранения на компоненте своего размещения;

2) сервис может использовать в качестве входной информации данные из другого компонента облачной среды без сохранения на компоненте своего размещения.

Переход предлагается осуществлять за счёт добавления в модель новых компонентов, функционирующих на облаке-источнике и облаке-получателе. В этом случае транспортный сервис будет принимать данные на одном облаке и создавать копию на другом. При осуществлении транспорта необходимо удостовериться, что *облако-получатель* имеет уровень безопасности, достаточный для хранения копии данных, которая наследует уровень конфиденциальности оригинала. В силу этих причин должно быть соблюдено правило: $l(p) \geq l(o)$. Если происходит нарушение приведенного условия, то, варианты, по которым происходит распределение рабочего процесса, перестают отвечать установленным требованиям безопасности и должны быть исключены из набора надёжных переходов. В итоге проверка на соблюдение формальных требований безопасности для вариантов размещения рабочего процесса из таблицы 1 не допускает использование более половины возможных вариантов. В результате шесть вариантов, не нарушающих требования безопасности, отражены в таблице 2.

Заключение

Для обеспечения безопасной обработки критичных данных в условиях среды облачных вычислений предложена модель безопасности процессов обработки данных, позволяющая на основании требований безопасности, распределить критические активы организации в *новую гибридную среду* облачных вычислений. Адаптирована классическая модель безопасности Белла-ЛаПадула с использованием ключевых элементов теории графов для определения формализованных требований безопасности облачных сервисов и данных.

Таблица 2

Допустимые варианты распределения рабочего процесса

№	Вариант
1	$o_1^1 \to t_1^1 \to o_2^1 \to передатчик \to o_2^0 \to t_2^0 \to o_3^0$
2	$o_1^1 \to t_1^1 \to o_2^1 \to передатчик \to o_2^0 \to t_2^0 \to o_3^0 \to передатчик \to o_3^1$
3	$o_1^1 \to t_1^1 \to o_2^1 \to передатчик \to o_2^0 \to передатчик \to o_2^1 \to t_2^1 \to o_3^1 \to передатчик$
4	$o_1^1 \to t_1^1 \to o_2^1 \to передатчик \to o_2^0 \to передатчик \to o_2^1 \to t_2^1 \to o_3^1$
5	$o_1^1 \to t_1^1 \to o_2^1 \to t_2^1 \to o_3^1 \to передатчик \to o_3^0$
6	$o_1^1 \to t_1^1 \to o_2^1 \to t_2^1 \to o_3^1$

Список литературы

1. Peter Mell, Timothy Grance. NIST Special Publication 800-145. The NIST Definition of cloud computing. 2011. 3 p.
2. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7. 2002. 1084 p.
3. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006, 176 с.
4. Bell, D. E. and LaPadula, L. J.: Secure Computer System: Unified Exposition and Multics Interpretation, Tech report ESD-TR-75-306, Mitre Corp, Bedford, Ma. (1976)
5. Харари Ф. Теория графов. Изд. 2-е. – М.:Едиториал УРСС, 2003. – 296 с.
6. Вдовин И. COBIT 4.1. Издательство: Аудит и контроль информационных систем. ISBN 978-5-9901321-1-5; 2008 г. 240 с.