УДК 004.056

А.Н. Волокита, Д.Т. Ву, И.В. Коханевич,А.Е. Бидков

МОДЕЛЬ ПОДДЕРЖКИ БЕЗОПАСНОСТИ РЕСУРСОВ CLOUD СИСТЕМ НА УРОВНЕ ИНФРАСТРУКТУРЫ

Аннотация: В статье рассматриваются основные угрозы облачных вычислений. Приведена типичная структура облачной системы, рассмотрены решения для защиты ее ресурсов. Описана обобщенная модель поддержки безопасности на уровне инфраструктуры.

Ключевые слова: модель поддержки безопасности, cloud computing, проблемы безопасности, структура облачной системы

Введение

Реализуя новый подход к предоставлению ИТ услуг, облачные системы подвержены традиционным компьютерным и сетевым проблемам безопасности, таким как обеспечение конфиденциальности, целостности и доступности. При этом возникают дополнительные угрозы, связанные с самой концепцией облачных вычислений [1].

Облачные вычисления предоставляют организациям возможность сократить затраты на ИТ, передать провайдеру управление инфраструктурой и сосредоточится на ключевых задачах организации. Например, согласно договору с объявленной стоимостью 200 миллионов долларов, подписанному в декабре 2011 года сроком на 10 лет, IBM будет отвечать за развитие и поддержку приложений и информационных систем ПАО “Укрсоцбанк”, а также управление ИТ-инфраструктурой банка.

В статье приведен анализ проблем безопасности cloud computing, показано способы решения отдельных задач, а также предложена модель безопасности cloud.

Проблемы безопасности облачных вычислений

На основании публикаций [2, 3] выделены основные угрозы безопасности облачных вычислений.

Несанкционированное использование облачных вычислений

Провайдеры предоставляют своим клиентам иллюзию неограниченных вычислительных и сетевых мощностей, а также безразмерного объёма хранилища. Получить доступ к данным ресурсам может любой зарегистрированный пользователь, что является значительной угрозой в случае нарушения лицензионного соглашения и правил использования облачных вычислений. Одним из примеров служит ботнет, распространяющий спам и вредоносное программное обеспечение. Злоумышленники, проникнув в публичный cloud, и используя мощности его инфраструктуры, распространяют вредоносное ПО и совершают атаки на тысячи других компьютеров.

© А.Н. Волокита, Д.Т. Ву, И.В. Коханевич,А.Е. Бидков, 2012

Безопасность взаимодействия провайдера и пользователя

Провайдеры облачных вычислений должны выполнять контроль аппаратных ресурсов, на которых запускаются гостевые ОС. Поэтому, при проектировании cloud, чрезвычайно важно учитывать возможные угрозы, возникающие при взаимодействии провайдера и пользователя, такие как: атаки исходящие от других клиентов, в результате разрушения барьера между пользователями, а также проблемы надежности и доступности.

Уязвимости аппаратного обеспечения

Совместное использование инфраструктуры является базовым принципом работы провайдеров cloud computing. При этом существует проблема безопасности, связанная с отсутствием изначальной поддержки аппаратного обеспечения. Для решения данной проблемы в cloud computing используется гипервизор, выступающий посредником между аппаратными ресурсами и гостевой операционной системой. Однако в гипервизоре присутствуют недостатки, которые потенциально могут позволить гостевым ОС получать несанкционированный доступ к аппаратной платформе.

Потеря или утечка данных

Потеря или утечка данных является важнейшей проблемой любой организации, поскольку это может привести не только к потере своей репутации, но и в некоторых случаях, к нарушению закона. Наглядным примером несанкционированного доступа к информации является изменение или удаления данных из виртуальной системы cloud computing без предварительного резервного копирования, а потеря ключа шифрования соизмерима с полной утратой информации. Кроме того, необходимо исключить любую возможность получения конфиденциальных данных сторонними лицами.

Большое количество анонимных учетных записей

Обновление кода, уязвимости профилей, попытки вторжения – это одни из важнейших факторов оценки безопасности системы. Вся информация о том, кто совместно использует систему, а также неудачные попытки аутентификации и атак должны быть зафиксированы в специальных журналах (логах).

Потенциально опасные программные интерфейсы

Провайдеры предлагают широкий набор программных интерфейсов (API) для взаимодействия клиентов с сервисами cloud. Безопасность и доступность основных сервисов “облака”, в том числе зависит и от безопасности программных интерфейсов, поскольку злоумышленники могут воспользоваться уязвимостями API для получения несанкционированного доступа к cloud.

 ISSN 1560-8956

Организационные каналы утечки

Угроза, исходящая от внутренних пользователей, является одной из основных причин, по которой большинство провайдеров не разглашают принципы приема на работу, доступа к данным и контроля рабочего персонала. Прозрачность этих процессов, жизненно важный аспект безопасности cloud computing. Кроме того, необходимо учитывать нормативные и правовые ограничения. Например, в большинстве стран информация, являющаяся государственной тайной, не может покидать пределы государства.

Типовые решения проблем поддержки безопасности

Структуру облачной системы на уровне инфраструктуры можно представить в виде объединения ресурсов: вычислительных серверов, хранилища данных и виртуальных образов (рис. 1). Ресурсы объединяются через внутреннюю сетевую инфраструктуру и управляются менеджером облачной системы.

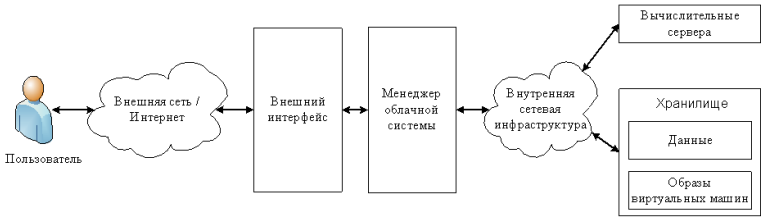

Рис. 1 – Структура типичной облачной системы

Для каждого ресурса требуется свой подход к обеспечению безопасности. Далее рассмотрены решения поддержки безопасности для хранилища образов [4], вычислительных серверов [5], а также менеджер конфиденциальности [6], который обеспечивает защищенное взаимодействие пользователя с облаком. Для хранилища данных и менеджера облачной системы реализуется поддержка менеджера конфиденциальности на стороне облачной системы.

Безопасность хранилища образов виртуальных машин

Совместное использование образов виртуальных машин приводит к появлению новых угроз безопасности для облачных вычислений. Угрозы могут проявляться как для владельцев образов, так и для их пользователей, а также для администраторов cloud.

Поддержка безопасности хранилища образов виртуальных машин, представленная на рис. 2, состоит из 5 основных компонентов:

- Система разграничения доступа - предоставление доступа к образам только пользователям, имеющим соответствующие полномочия от владельца.

- Блок фильтров – фильтрация информации при публикации образа, а также при его использовании. При публикации фильтры позволяют удалить или скрыть данные, нежелательные для распространения, из исходного образа.
- Блок управления безопасностью – общая координация всех компонентов хранилища образов виртуальных машин, а также реализация механизма отката к предыдущим версиям.
- Блок контроля целостности – периодическое сканирование опубликованных образов для обнаружения возможных угроз и их устранения.
- Репозиторий образов виртуальных машин – хранение образов виртуальных машин с возможностью ведения истории изменений для каждого из пользователей.

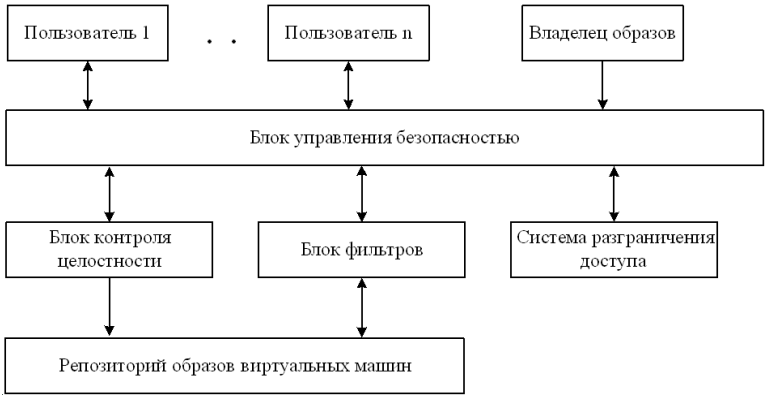

Рис. 2 – Хранилище образов виртуальных машин

Преимущества. Фильтры позволяют уменьшить риски публикации личных данных, а также вредоносного ПО. Система хранит изменения предоставляющие возможность при необходимости, откатиться к предыдущим версиям. Контроль доступа предотвращает использование образов виртуальных машин без соответствующих прав.

Недостатки. Огромные вычислительные и временные затраты. Пользователь не может полностью устранить все риски, поскольку фильтры не являются точными на 100%. Антивирусное сканирование не всегда обнаруживает все вредоносное ПО, слежение и контроль за данными пользователя повышает ответственность поставщиков услуг.

Менеджер конфиденциальности на стороне клиента

Менеджер конфиденциальности (рис. 3) позволяет снизить риски утечки и потери конфиденциальных данных в облачных системах, а

 ISSN 1560-8956

также предоставляет дополнительные возможности, связанные с безопасностью.

Основные особенности:

- Обфускации – позволяет скрывать часть или всю структуру данных перед передачей в облако, а также производить обратные действия над данными, полученными из облака.
- Управления привилегиями - позволяет пользователю задавать настройки обращения со своими данными, хранящимися в открытом виде.
- Доступ к данным аудита – обеспечивает доступ к личной информации пользователя в облаке, содержащей данные аудита, что позволяет обнаружить нарушение конфиденциальности.
- Обратная связь – позволяет пользователю получать информацию, связанную с использованием его данных.
- Управление ролями – позволяет пользователю выбирать роль при взаимодействии с облаком.

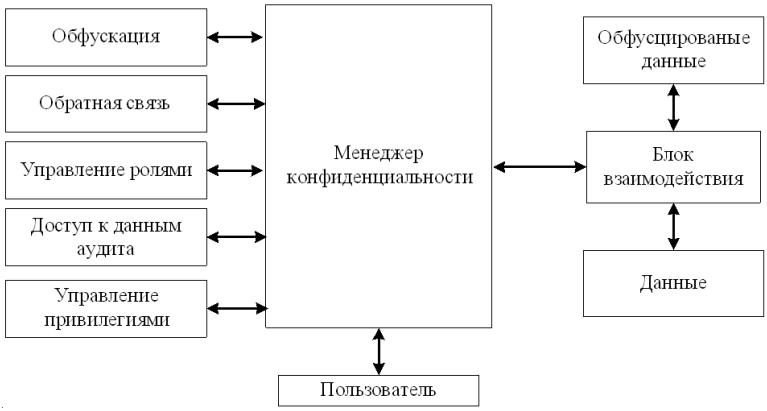

Рис. 3 – Использования менеджера конфиденциальности

Преимущества. Позволяет снизить риски утечки и потери конфиденциальных данных, контролировать использование данных, а также проводить аудит.

Недостатки. Для использования менеджера конфиденциальности необходима поддержка его возможностей со стороны облачного сервиса.

Промежуточная система защиты облачных вычислений

Промежуточная система защиты облачных вычислений предназначена для мониторинга целостности компонентов cloud computing. Данное решение призвано защитить целостность гостевых виртуальных

машин, а также распределенного промежуточного программного обеспечения, что дает возможность хост-платформе контролировать гостевые виртуальные машины и компоненты инфраструктуры.

На рис. 4 изображена обобщенная структура данного решения. Промежуточная система защиты облачных вычислений – это промежуточное ПО, ядро которого размещено между ядром ОС и слоем виртуализации. Используя либо пассивный, либо активный мониторинг, данная система может определять любую возможную модификацию в данных и коде ОС, что гарантирует целостность ядра ОС и промежуточного ПО “облака”.

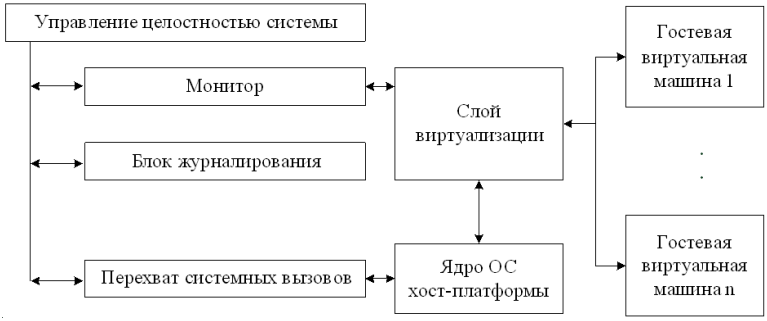

Рис. 4 – Промежуточная система защиты облачных вычислений.

Преимущества. Является “прозрачной” со стороны гостевой виртуальной машины. Может быть развернута на большинстве доступных промежуточных ПО. Обнаруживает попытки вторжения на гостевые машины и, если это требует политика безопасности, предпринимает соответствующие действия в отношении злоумышленника и/или уведомляет удаленный компонент защиты промежуточного ПО.

Недостатки. Необходимость установки дополнительного ПО на хост машины. Задержки, связанные с перехватом системных вызовов. Решение не защищает от всех видов угроз.

Обобщенная модель поддержки безопасности облачных вычислений на уровне инфраструктуры

Cloud предоставляет три основных типа ресурсов: хранилище образов виртуальных машин, набор вычислительных серверов, на которых они могут быть запущены, а также массив хранилищ данных.

Построим таблицу покрытия задач поддержки безопасности рассмотренными ранее решениями (табл. 1).

В строках таблицы представлены задачи поддержки безопасности, а в столбцах – рассмотренные выше способы.

Безопасность инфраструктуры – безопасность разных уровней “облака”, в основном, сетевого уровня, уровня хост-платформы, а также уровня прикладных программ.

Таблица 1

Таблица покрытия задач поддержки безопасности облачных систем

Задачи	Хранилище образов виртуальных машин	Менеджер конфиденциальности	Промежуточная система защиты облачных вычислений
Безопасность инфраструктуры	+	-	+
Безопасность данных	+	+	+
Управление идентификацией и контроль доступа	+	+	-
Управление безопасностью	+	+	-
Конфиденциальность	+	+	-
Аудит	+	+	+
Безопасность как сервис	-	+	-

Из таблицы видно, что описанные ранее решения по-отдельности не обеспечивают полноценное покрытие задач поддержки безопасности cloud computing. Более того, покрытие нельзя считать эквивалентным, так как выполняемые задачи относятся к разным частям облачной системы.

Для разрешения данной ситуации возможна интеграция представленных решений в единую модель (рис. 5). Как видно из рисунка, обобщенная модель повторяет типичную структуру, представленную на рис. 1.

Вся информация об использовании ресурсов хранится в общем блоке мониторинга. Пользователь имеет доступ к тем данным мониторинга, которые непосредственно связаны с ним.

Менеджер конфиденциальности обеспечивает безопасность взаимодействия пользователя и облака, поддерживая шифрование и предоставляя дополнительные возможности по управлению правами доступа и контролю данных. Поддержка взаимодействия обеспечивается с помощью менеджера облачной системы. Блок контроля доступа к данным разграничивает доступ к данным пользователя и предоставляет информацию об их использовании.

Образы виртуальных машин хранятся в специальном хранилище, которое поддерживает систему контроля версий. Данное хранилище защищено с помощью системы разграничения доступа, блока контроля целостности, а также фильтров. Взаимодействие с хранилищем происходит через блок управления безопасностью.

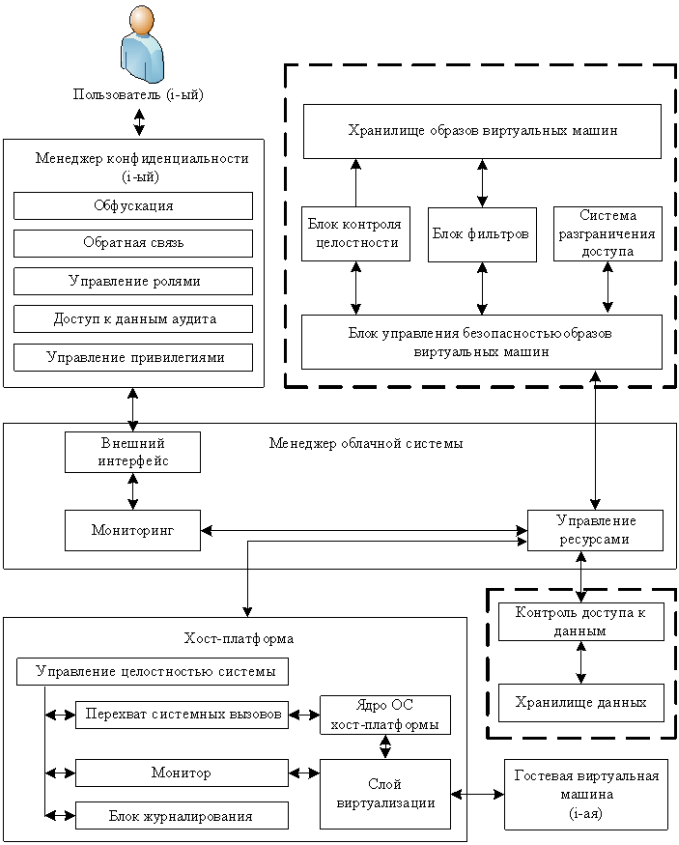

Рис. 5 – Обобщенная модель поддержки безопасности облачных вычислений.

При запуске гостевой ОС, образы виртуальных машин загружаются из хранилища на хост-платформу. Мониторинг системы происходит на протяжении всего времени работы, все потенциально опасные события заносятся в специальные журналы.

Выводы

Вопрос безопасности является ключевой проблемой в cloud computing. В данной статье были рассмотрены основные угрозы облачных вычислений, а также способы их решения. Было определенно, что данные методы не обеспечивают полноценную защиту cloud computing. Исходя из этого, возникает необходимость их интеграции в рамках единой си-

стемы. Данная система состоит из набора подсистем, каждая из подсистем отвечает за отдельное направление обеспечения безопасности.

Стоит также учитывать, что не все проблемы могут быть полностью решены программно-техническими средствами, так как система защиты включает в себя и организационно-технические мероприятия.

Литература

1. Badger Lee, Grance Tim, Patt-Corner Robert, Voas Jeff. DRAFT Cloud Computing Synopsis and Recommendations Special Publication 800-146, May 2011.
2. Srinivasamurthy Shilpashree, Liu David Q.. Survey on Cloud Computing Security.
3. Hubbard Dan, Sutton Michael etc. Top Threats to Cloud Computing V1.0. Cloud Security Alliance, March 2010.
4. Wei Jinpeng, Zhang Xiaolan, Ammons Glenn, Bala Vasanth, Ning Peng, Managing Security of Virtual Machine Images in a Cloud Environment. CCSW ’09: Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96. November 2009.
5. Mowbray Miranda, Pearson Siani. A Client-Based Privacy Manager for Cloud Computing. COMSWARE ’09: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middleware . June 2009.
6. Lombardi Flavio, Di Pietro Roberto. Transparent Security for Cloud. SAC ’10: Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415. March 2010.

Отримано 14.11.2012 р.