Д. С. Симоненкова, А. Н. Велигура

ЭТАЛОННЫЕ МОДЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В настоящее время технологии облачных вычислений развиваются стремительными темпами, появляются новые облачные платформы и услуги. Для обеспечения безопасности данных в облаке должны быть определены требования к системе защиты, а для этого должна быть построена детализированная модель угроз безопасности сред облачных вычислений. К сожалению, методики построения модели угроз информационной системы, построенной на основе технологий облачных вычислений (ИСОТ) на момент написания данной статьи в литературе найти не удалось. Для построения модели угроз ИСОТ необходимо описать структуру самой системы, для чего был проведен анализ различных моделей ИСОТ по версии NIST, IBM и Microsoft.

Эталонная модель ИСОТ по версии NIST

Эталонная модель высокого уровня облачных вычислений по версии NIST [1] представлена на рис. 1.

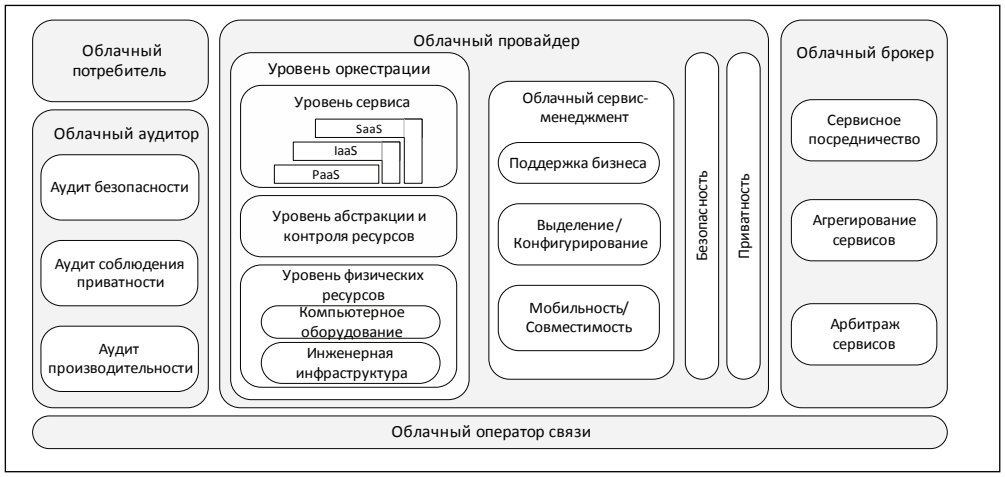

Рис. 1. Эталонная модель ИСОТ по версии NIST

Эталонную модель облачных вычислений по версии NIST определяют пять основных участников: оператор облака, аудитор облака, облачный брокер, облачный оператор связи, подписчик облака.

В данной модели ИСОТ можно выделить следующие уровни.

Уровень оркестрации поддерживается оператором облака для организации деятельности по координации и управлению вычислительными ресурсами, для обеспечения подписчиков облака требуемыми сервисами.

Уровень сервиса определяет базовые сервисы (SaaS, PaaS, IaaS), предоставляемые оператором облака.

Уровень абстракции и контроля ресурсов содержит компоненты системы, которые оператор облака использует для предоставления и управления доступом к физическим вычислительным ресурсам через абстракции ПО, например, гипервизор, виртуальные машины (ВМ), виртуальные хранилища данных и другие абстракции вычислительных ресурсов, используемые для реализации облачной инфраструктуры. Абстракция ресурсов должна обеспечивать эффективность, безопасность и надежность использования основных физических ресурсов. Функция контроля

ресурсов относится к компонентам ПО, которое является ответственным за распределение и контроль использования ресурсов, а также за управление доступом.

Уровень физических ресурсов включает в себя компьютерное оборудование и инженерную инфраструктуру.

Компьютерное оборудование содержит аппаратные ресурсы, такие как компьютеры (CPU и память), сеть (роутер, МСЭ, коммутатор, сетевые каналы и интерфейсы), компоненты хранения (жесткие диски) и другие физические элементы вычислительной инфраструктуры.

Инженерная инфраструктура состоит из отопления, вентиляции, системы кондиционирования и питания, коммуникаций и других элементов физической площадки размещения компьютерного оборудования.

Облачный сервис-менеджмент включает все связанные с сервисом функции, необходимые для управления, функционирования сервисов, требующихся подписчикам облака. Облачный сервис-менеджмент может быть описан с точки зрения поддержания бизнеса, выделения и конфигурирования ресурсов, мобильности и совместимости.

Безопасность облачной системы охватывает все слои эталонной модели, от физической безопасности до безопасности приложений. В рамках обеспечения безопасности ИСОТ рассматриваются: аутентификация и авторизация подписчиков облака, выделение и назначение ресурсов для восстановления, обновления и подключения новых узлов, мониторинг виртуальных ресурсов, мониторинг функционирования облака и генерация отчетов о производительности, предоставление возможностей количественных измерений на уровне абстракции, определение параметров соглашения об уровне предоставления услуги (Service Level Agreement (SLA)), мониторинг выполнения SLA в соответствии с заданными политиками и управление политикой безопасности.

Эталонная модель ИСОТ по версии Microsoft

Эталонная модель ИСОТ, предложенная компанией Microsoft [2], является попыткой детализировать программно-аппаратную составляющую ИСОТ. В данной модели выделены восемь уровней. Иерархия уровней представлена на рис. 2.

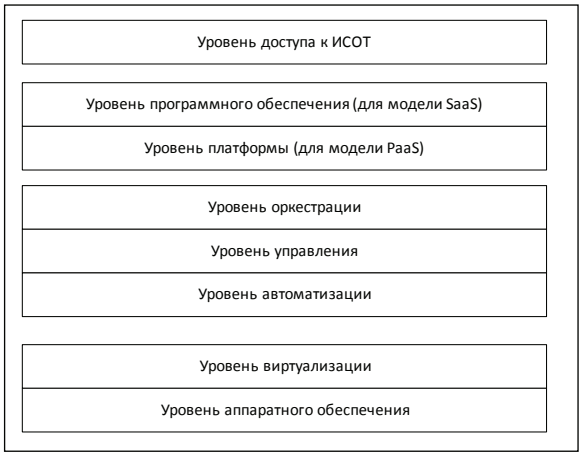

Рис. 2. Иерархическая эталонная модель ИСОТ

Уровень аппаратного обеспечения объединяет аппаратное обеспечение, используемое для оказания услуг подписчикам ИСОТ (серверное оборудование, телекоммуникационное оборудование, системы хранения данных и т. п.).

Уровень виртуализации абстрагирует физические аспекты реализации вычислительных ресурсов, представляя их вышестоящим уровням в виде виртуальных машин — совокупности технических характеристик вычислительного ресурса и информации, хранимой на дисковом пространстве.

Уровень автоматизации реализует программный интерфейс для выполнения операций над виртуальными машинами (создание, изменение, запуск, остановка).

На уровне управления реализуются основные функции управления виртуальными машинами, предлагаемые подписчикам. Как правило, здесь же реализуются основные функции безопасности ИСОТ, связанные с управлением доступом подписчиков к вычислительным ресурсам.

Уровень оркестрации предназначен для унификации функций управления вычислительными ресурсами ИСОТ в тех случаях, когда в пределах одного облака для нижестоящих уровней используются разные программные решения.

Уровень платформы необходим для модели предоставления услуг PaaS и может быть востребован в модели предоставления услуг SaaS.

Уровень программного обеспечения необходим только для модели предоставления услуг SaaS и фактически реализует прикладное программное обеспечение оператора, которому передаются на обработку пакеты исходных данных подписчиков.

В модели предоставления услуг IaaS два последних уровня не реализуются.

На уровне доступа к ИСОТ реализуются протоколы удаленного доступа к функциям ИСОТ.

Эталонная модель ИСОТ по версии IBM

Эталонная модель ИСОТ по версии IBM [3] представлена на рис. 3.

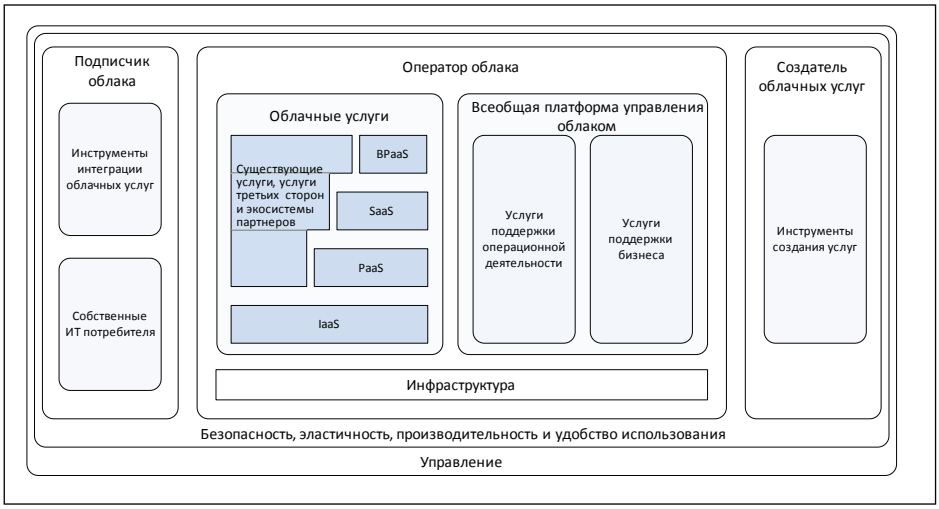

Рис. 3. Эталонная модель ИСОТ по версии IBM

В соответствии с рис. 3, модель ИСОТ может быть определена тремя главными ролями (подписчик, оператор и создатель облачных услуг), каждая из которых может выполняться отдельным субъектом, группой субъектов или организацией.

В контексте эталонной архитектуры облачных вычислений IBM модели облачных сервисов могут быть выделены четыре модели: IaaS, PaaS, SaaS или BPaaS. Первые три модели описаны в [4], последняя модель определена в рамках эталонной архитектуры IBM.

BPaaS — это любой бизнес-процесс, который предоставляется как облачный сервис через Интернет и, соответственно, поставщик BPaaS несет ответственность за определенные бизнес-функции.

Инфраструктура представляет все элементы инфраструктуры оператора облака, которые необходимы для предоставления облачных сервисов (сервера, системы хранения и сетевые ресурсы, подключение этих ресурсов, размещенных в центре обработки данных и т. д.).

Всеобщая платформа управления облаком предоставляет набор бизнес-услуг и услуг, ориентированных на управление использованием сервисов.

Функции платформы управления доступны через API, обеспечиваемые внутренними компонентами платформы. Платформа предоставляет услуги, которые могут быть использованы в контексте конкретной облачной услуги.

Бизнес-услуги — это множество связанных с бизнесом услуг, которые предоставляются платформой управления облаком и необходимы создателю облачных услуг для реализации облачных сервисов.

Служба поддержки эксплуатации представляет собой набор технических услуг, предоставляемых платформой управления, которые необходимы создателю облачных услуг для реализации облачных сервисов.

Безопасность, отказоустойчивость, производительность являются сквозными аспектами, которые охватывают всеобщую платформу управления облаком, аппаратную инфраструктуру и облачные услуги.

Инструменты создания услуг используются создателем облачных услуг для разработки новых сервисов (сервисы мониторинга, изменения и обновления, корпоративные приложения, схемы баз данных и т. д.).

Построение эталонной модели ИСОТ

В рассмотренных выше моделях уровни виртуализации и сервисов не детализированы. В то же время, как представляется, при построении модели угроз данные уровни играют главную роль. Ввиду этого предлагается новая модель ИСОТ, которая детализирует компоненты, входящие в данные уровни. Новая модель ИСОТ представлена на рис. 4.

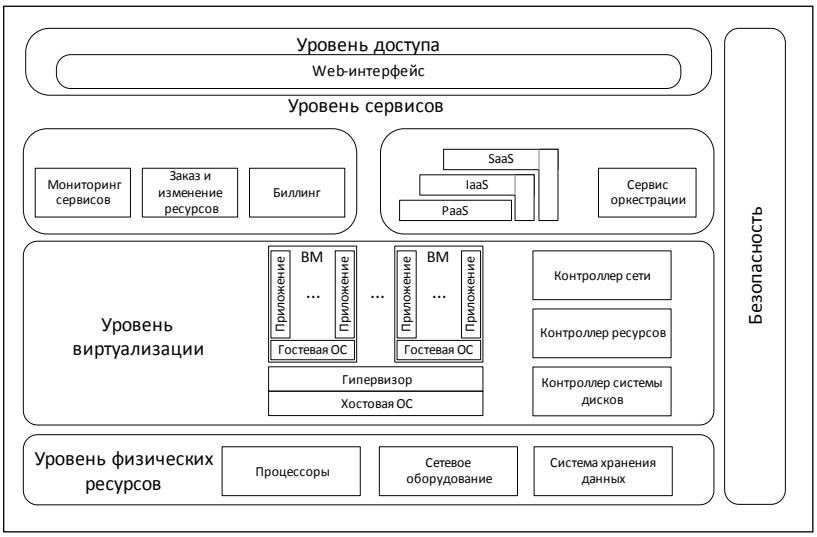

Рис. 4. Предлагаемая эталонная модель ИСОТ

Предлагаемая модель облачных вычислений содержит два главных действующих субъекта: подписчик облака и оператор облака. В данной модели ИСОТ могут быть выделены следующие уровни.

На уровне доступа к ИСОТ осуществляется предоставление доступа администраторам к функциям управления ИСОТ и подписчикам облака к функциям самообслуживания.

На уровне сервисов оператором облака предоставляются такие услуги, как IaaS, SaaS и PaaS. Уровень включает в себя сервис оркестрации, который выполняет функции мониторинга, управления, планирования вычислительных ресурсов и ресурсов хранения данных. На этом уровне осуществляется управление предоставляемыми услугами (выделение, доставка и т. д.).

Уровень виртуализации является основным уровнем, благодаря которому физические ресурсы превращаются в виртуальные машины, сети и диски для хранения данных. На этом уровне осуществляется контроль виртуальных ресурсов.

Уровень физических ресурсов включает в себя все вычислительные ресурсы, системы хранения данных и сетевое оборудование, располагаемое в центре обработки данных.

Уровень безопасности обеспечивает безопасность архитектуры и охватывает все уровни модели ИСОТ.

Таким образом, в предложенной модели более детально рассмотрены уровни виртуализации и сервисов, и данная модель может быть использована для дальнейшего представления ИСОТ с использованием сетей Петри при разработке методики построения модели угроз.

СПИСОК ЛИТЕРАТУРЫ:

1. NIST SP 500-292 NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology. U.S. 2011.
2. Построение архитектуры частного облака от Microsoft. [Электронный ресурс]. URL: http://www.winzone.ru/articles/1047 (дата обращения: 21.08.2013).
3. Introduction and Architecture Overview. IBM Cloud Computing Reference Architecture. [Электронный ресурс]: Document version 2.0 — 28 January 2011. URL: https://s3-sa-east1.amazonaws.com/bucketmanoelveras/manoel_veras_PROFESSIONAL/CLOUDCOMPUTING/Artigos/Artigos_IBM/arq_ibm.pdf (дата обращения: 21.08.2013).
4. NIST SP 800-145 The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. U.S. 2011.