УДК 681.3

МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ОБЛАЧНЫХ СЕРВИСОВ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМОВ ВИРТУАЛИЗАЦИИ

Алексей Алексеевич РЫБАЛКО родился в 1984 г. в городе Москве. Аспирант МАИ. Основные научные интересы — в области компьютерного моделирования, компьютерной графики, компьютерной безопасности. Автор шести научных работ. E-mail: ar@aagern.com

Alexey A. RYBALKO was born in 1984, in Moscow. He is a Postgraduate Student at the MAI. His research interests are in computer simulation, computer graphics, computer security. He has published 6 technical papers. E-mail: ar@aagern.com

Работа посвящена вопросам моделирования систем защиты сетевого периметра центров обработки данных (ЦОД) с использованием механизмов виртуализации. Приведен общий обзор выбранной методики и инструментальных средств защиты. Произведено построение диаграммы прецедентов, диаграммы последовательности и диаграммы состояний с помощью языка моделирования UML. Предложены методы математического обобщения системы безопасности с элементами виртуализации и центром управления.

The following work is dedicated to modeling the perimeter network security systems of datacenters. The work is focused on the usage of virtualization mechanisms to provide protection of web servers and cloud based applications. A base analysis is made of methodology and instruments chosen for the task. Also, the UML programming language is used for making the basic modeling: use case diagram, sequence diagram and the state diagram.

Ключевые слова: виртуализация, диаграмма состояний, диаграмма последовательности, диаграмма прецедентов, диаграмма состояний, отказоустойчивость системы, компьютерная безопасность.

Key words: virtualization, use case diagram, sequence diagram, state diagram, computer security, system failover.

Введение

Механизмы изоляции программных приложений для последующего анализа давно применяются в системах компьютерной безопасности (СКБ). Однако сложность эффективного применения данных механизмов заключается во все возрастающей тенденции приложений к сетевому взаимодействию между собой с использованием удаленных ресурсов, а также в подключении удаленных абонентов. С появлением принципиально новых приложений в рамках систем облачных вычислений требуется внести изменения в традиционный подход к обеспечению безопасности, поиск новых, более гибких и в то же время надежных СКБ.

Современные методы защиты приложений в большей степени эвристические, а их проактивная составляющая обычно ограничивается вариациями сигнатур. Бурное развитие виртуализации настольных ПК, сначала с программной, а затем и с программно-аппаратной поддержкой, обеспечило мощный механизм эффективной изоляции приложений. В совокупности с традиционными моделями СКБ стало возможным говорить о новом подходе к организации защиты как отдельных компьютеров, так и локальных вычислительных сетей. Таким образом, возрастает не только надежность, но и безопасность функционирования приложений [1].

Рассмотрим современные задачи по удаленному взаимодействию сетей, надежности и безопасности такого взаимодействия. Сегодняшняя тенденция, в будущем обещающая стать общемировой практикой, — это размещение бизнес-приложений, отдельных служб или целиком инфраструктуры компании на удаленных ЦОД с последующим управлением через Интернет. Такая тенденция получила название «облачные вычисления» и делится на следующие основные варианты:

Software as a Service (*SaaS*) — схема подачи ПО, при которой поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя заказчикам доступ к программному обеспечению через Интернет. Основное преимущество модели SaaS для потребителя состоит в отсутствии затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и программного обеспечения, работающего на нём.

Platform as a Service (*PaaS*) — схема предоставления интегрированной платформы для разработ-

ки, тестирования, развертывания и поддержки веб-приложений как услуги.

Infrastructure as a Service (*IaaS*) — схема предоставления компьютерной инфраструктуры как услуги. Состоит из аппаратных средств, таких, как серверы, системы хранения данных, сетевое оборудование, операционных систем и системного ПО, а также связующего ПО.

Communication as a Service (*CaaS*) — схема подразумевает, что в качестве сервисов предоставляются услуги связи, например, IP-телефония, почта и мгновенные коммуникации (чат, Интернет-пейджеры и т.д.) [2].

Вне зависимости от модели предоставления облачных услуг, защита их со стороны поставщика сводится к защите ЦОД с размещенными на нем облачными приложениями, доступного из внешней сети. Основные критерии работы подобного ЦОД: круглосуточная доступность без перерывов в работе; защищенность от несанкционированного доступа, проникновения вредоносного ПО, аппаратных сбоев, а также возможность восстановления в случае аварии за минимальный промежуток времени [1].

Инструментарий защиты

Для решения задачи защиты ЦОД от вредоносного ПО, программных и аппаратных ошибок предлагается использовать в качестве инструментария технологию паравиртуализации на базе гипервизора Microsoft Hyper-V, так как в этом случае гостевая система обладает более высокой производительностью, реализуется полная поддержка драйверов оборудования хостовой ОС, поддержка многопроцессорных и многоядерных систем, тонкая настройка доступных для гостевых систем ресурсов (ОЗУ, распределение загрузки ядер(процессоров) и др.), а также простая система отслеживания работы виртуальных разделов [3]. Для автоматизированного управления гипервизорами MS Hyper-V, отслеживания возможных сбоев в виртуальной инфраструктуре и программировании реакции на них предлагается воспользоваться инструментарием Microsoft System Center Virtual Machine Manager (SCVMM), с расширением его функции с помощью языка Powershell. SCVMM позволяет развертывать и управлять набором виртуальных машин через единую консоль. С помощью языка Powershell можно расширить возможности SCVMM, разработав сценарии повышения безопасности и надежности решения: реакции на возникновение сбоев в работе виртуальных машин, на попытки атаки на виртуальную среду и другие внештатные ситуации [4].

Для повышения надежности рассматриваемой схемы хранение сценариев виртуализации и промежуточных данных об их состоянии построено на решении резервного копирования/восстановления Microsoft System Center Data Protection Manager (SCDPM) 2007 SP2 [6]. Асинхронная репликация, в случае аппаратных сбоев или атак, жертвами которых стали виртуальные машины внешнего контура защиты сети ЦОД, базируется на технологии Double-Take [7].

Общая схема защиты

Общая схема защиты корпоративной зоны безопасности представлена на рис. 1.

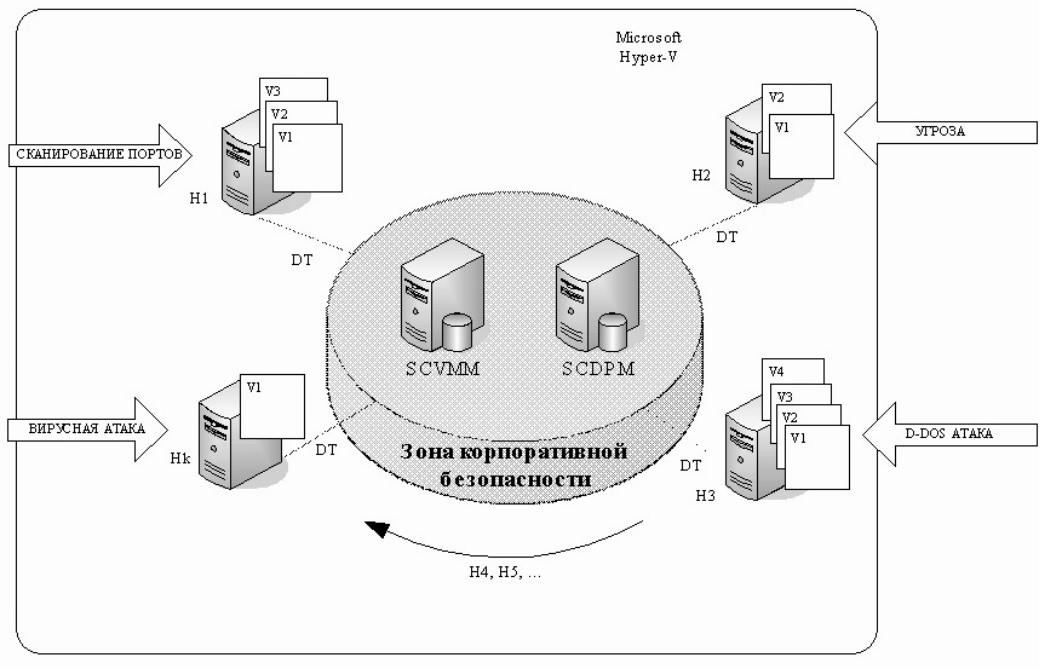

Рис. 1. Архитектура централизованного управления безопасностью

Пусть R — конечное (расширяемое) множество ресурсов корпоративной сети, которые допускают тонкую настройку виртуальных серверов для хостов H в контуре управления Hyper-V; S — набор сервисов, которые могут быть запущены на виртуальных серверах [3]. Тогда $R \times S$ — множество допустимых сценариев конфигурирования виртуализации. Если на внешнем периметре корпоративной сети расположены k физических серверов (рис. 1) различной архитектуры (H_l, $l = 1,k$), то по технологии Hyper-V на каждом из них могут быть запущены виртуальные машины (V_i^j) , управляемые из зоны корпоративной безопасности [5].

Объектное моделирование системы защиты

Для формализации задачи и моделирования системы защиты был использован унифицированный язык моделирования UML, с помощью которого был построен ряд диаграмм.

Диаграмма прецедентов — диаграмма, на которой отражены отношения, существующие между актерами и прецедентами. Основная задача — представлять собой единое средство, дающее возможность обсуждать функциональность и поведение системы. Диаграмма прецедентов системы защиты показана на рис. 2. Данная диаграмма представляет следующую структуру действующих лиц и сервисов, которые они контролируют:

• действующие лица: системный администратор, сервер управления виртуальной средой на базе System Center Virtual Machine Manager (SCVMM), локальная виртуальная машина — в данном случае это Hyper-V гипервизор виртуальной машины;

• сервисы делятся по действующим лицам, которые их исполняют:

◊ администратор осуществляет включение и выключение узлов системы, наблюдает за работой серверов, формирует отчетность на основе собранной статистики работы. Также администратор имеет право вносить изменения в работу системы путем программирования новых алгоритмов и изменения логики их исполнения — как инцидентной, так и по временному плану;

◊ управляющий сервер SCVMM хранит текущий план работы из набора, заданного администратором, на основе которого он осуществляет управление виртуальной инфраструктурой. SCVMM выполняет по шагам текущий план в соответствии с заданными временными метками, а также осуществляет выбор дальнейших шагов по плану в случае наличия ветвлений. SCVMM систематически запрашивает статусы подконтрольных виртуальных машин, анализирует на предмет ошибок или существенных отклонений от нормальной работы и, при наличии каких-либо сбоев, подключает ситуационные планы работы из заданного администратором набора;

◊ виртуальная машина получает команды от SCVMM, в соответствии с которыми осуществляет запуск, перезагрузку или отключение гостевых систем, отработку сценариев преодоления сбоев, а также систематический опрос статусов гостевых систем и размещенных на них серверных приложений.

Диаграмма последовательности — диаграмма, на которой изображено упорядоченное во времени взаимодействие объектов. В частности, на ней изображены участвующие во взаимодействии объекты и последовательность сообщений, которыми они обмениваются. Диаграмма последовательности системы защиты показана на рис. 3. Объектами данной диаграммы являются вредоносный код или атака вредоносного кода, атакуемое приложение, гостевая система, система предоставления и управления локальной виртуализацией (гипервизор), система управления виртуальной инфраструктурой (SCVMM) и база отчетов.

При выявлении атаки вредоносного кода на приложение оно пытается передать статусную информацию ОС (повышение уровня загруженности виртуального процессора, возникновение помех в работе и т.д.). ОС сохраняет полученную информацию как часть своего общего статуса, информация о котором затем передается локальному гипервизору и далее по запросу передается на SCVMM, который анализирует и записывает отчет в базу отчетности. Развернутые на гостевой системе приложения пытаются бороться с возникшей угрозой и продолжать нормальное функционирование, периодически передавая ОС обновленные статусы своей работы. В случае возникновения ошибок в работе приложения информация об этом поступает на ОС, которая подает ответную команду на перегрузку приложения. В случае возникновения повторных ошибок приложения, невозможности его перезагрузки, а также сбоев в гостевой ОС информация об этом поступает на локальный гипервизор, который санкционирует перезагрузку гостевой ОС. Информация об ошибках любого уровня поступает на SCVMM, анализируется и записывается в базу отчетности. В случае накопления ошибок приложений на гостевой ОС, повторных ошибок самой ОС, тяжелых сбоев в ее работе по команде от SCVMM локальный гипервизор производит принудительное отключение гостевой системы. После отключения

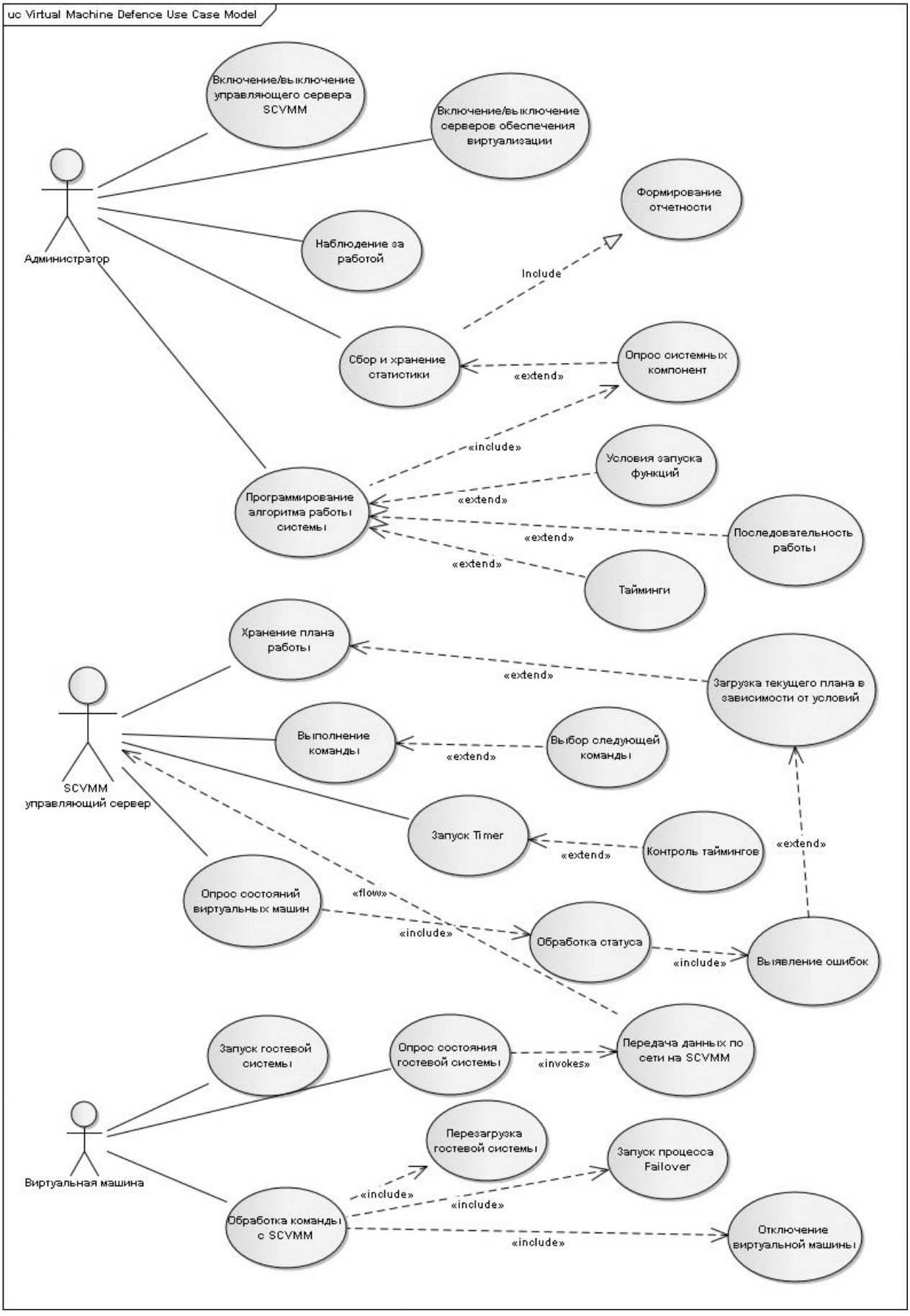

Рис. 2. Диаграмма прецедентов модели защиты

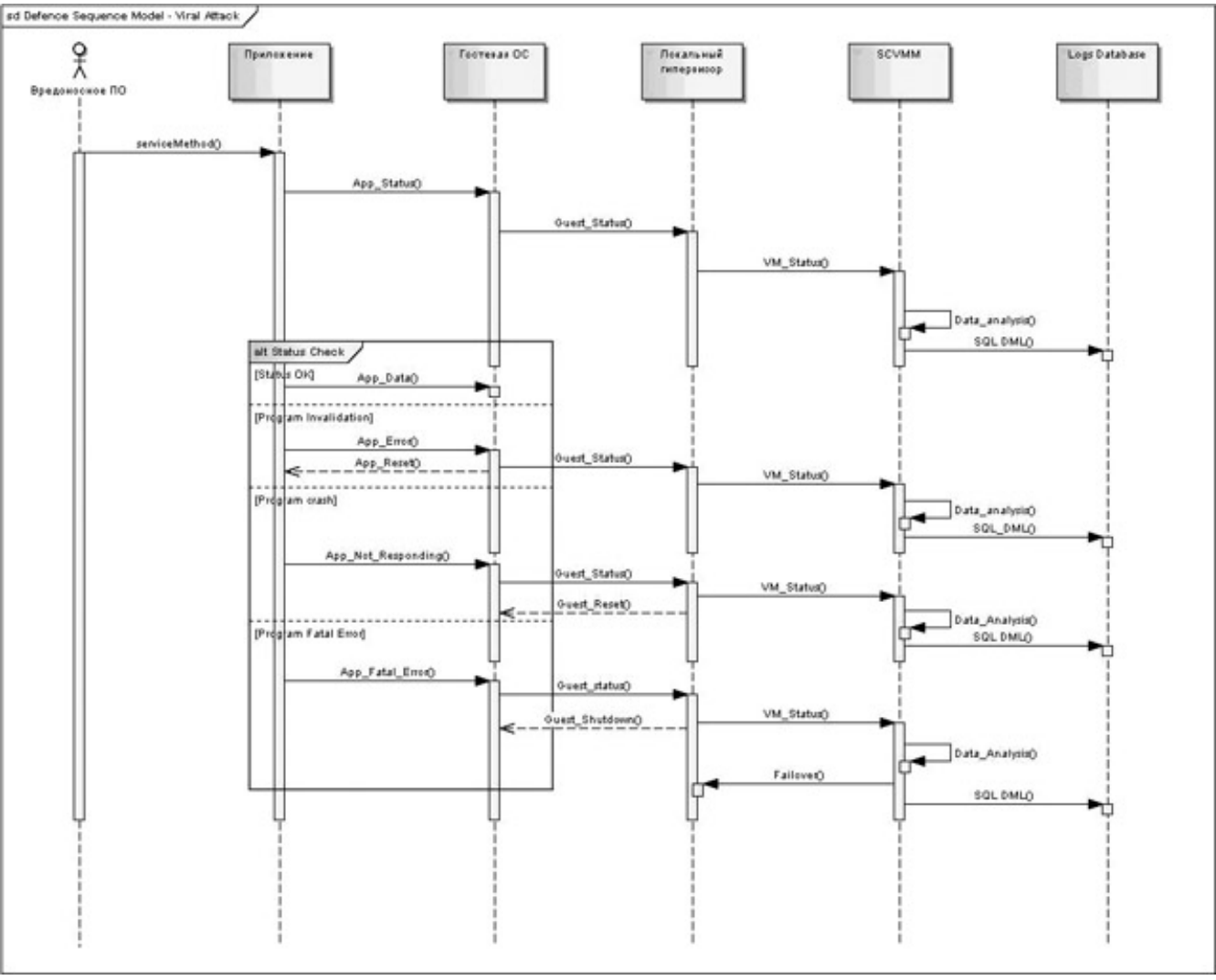

Рис. 3. Диаграмма последовательности модели защиты

производится процедура преодоления сбоев Failover() — уничтожение отработавшей ОС, создание и подключение нового готового образа гостевой ОС и ее приложений из библиотеки шаблонов, выделение ресурсов на работу новой системы и переключение пользователей на работу с ней.

Диаграмма состояний — диаграмма, на которой представлен конечный автомат с простыми состояниями, переходами и композитными состояниями. Диаграмма состояний системы защиты показана на рис. 4. Диаграмма показывает различные состояния системы и разделена на пять категорий по передаче управления:

1) администратор — в начальном состоянии осуществляет проверку работы системы. Осуществляет анализ отчетности, а также переключает систему в режим ручного управления;

2) SC VMM управляющий модуль — принимает данные от администратора или гипервизоров, формирует по принятым данным отчет, формирует список задач на языке Powershell для гипервизоров в зависимости от входных данных;

3) БД отчетности — осуществляет запись, а также обновление отчетной информации для последующего чтения в случае надобности в детальном анализе работы системы за заданный период времени;

4) локальный гипервизор — принимает данные от гостевых виртуальных машин (ВМ) и передает на обработку в SC VMM. Исполняет команды SC VMM и передает отчет об их успешной работе или о сбое;

5) гостевая ВМ — в начальном состоянии создает отчеты по статусу своей работы. В случае возникновения ошибок или сбоев принимает от гипервизора инструкции для ответной реакции и формирует отчет об успешности отработки данных инструкций.

Выводы

В качестве прикладной экспериментальной площадки для использования виртуализации в задачах

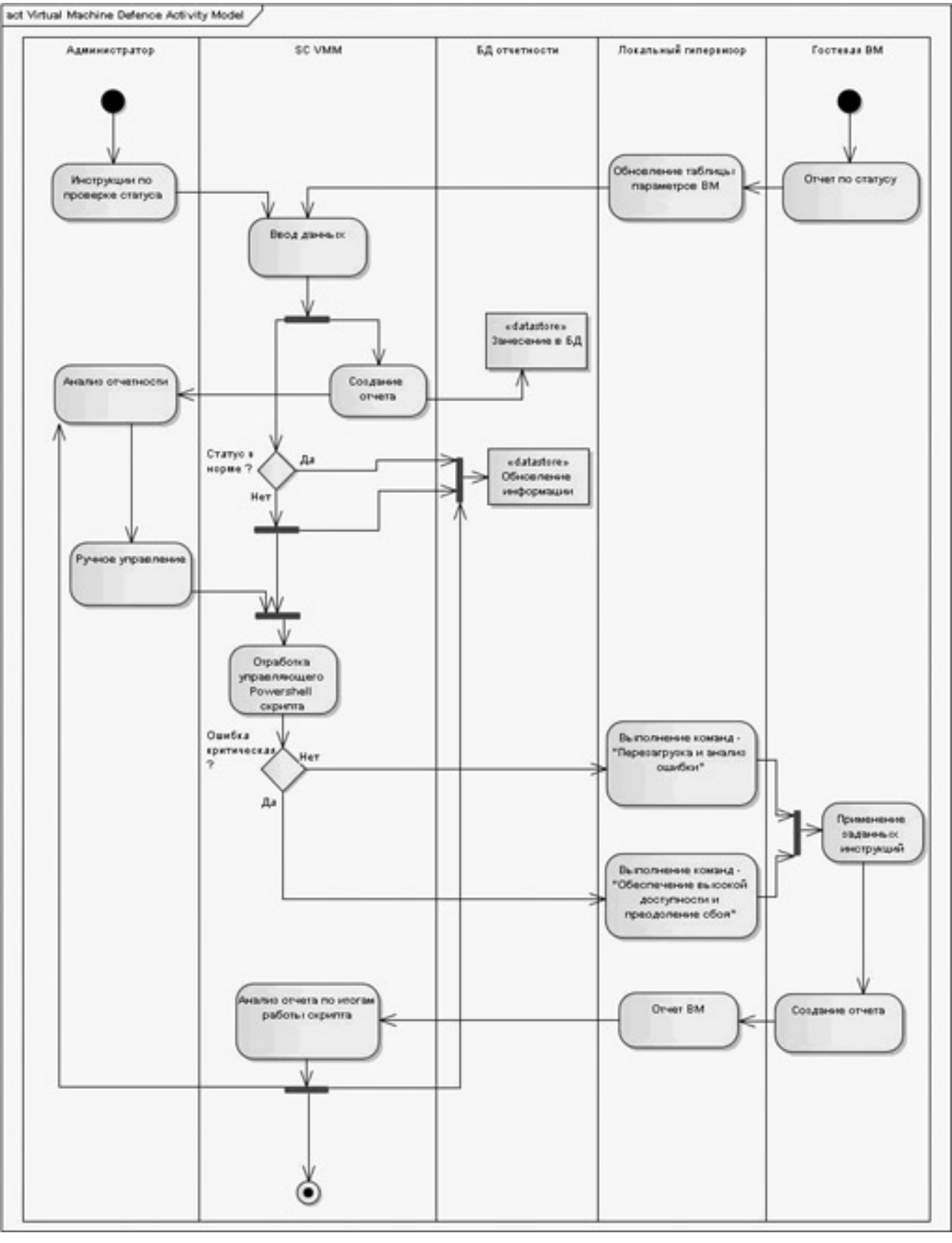

Рис. 4. Диаграмма состояний узлов защиты

комплексной защиты ЦОД был рассмотрен совместный центр решений компаний ООО «Кварта Технологии» и Microsoft [8]. Центр решений включает в себя систему по предоставлению CaaS сервисов на базе технологии Microsoft Unified Communications. Модульная система, развернутая на серверах центра решений, включает подсистему предоставления IP-телефонии, а также видеоконференций Microsoft Office Communications Server 2007 R2, сервер передачи голосовой и электронной почты Microsoft Exchange 2010, подсистему сбора статистики на основе сетевой базы данных Microsoft SQL 2008 и подсистему отслеживания состояния текущих соединений. Внутренняя безопасность и закрытость данных системы обеспечивается разделением ее пользователей по ролям, обусловленным проводимыми действиями и запрашиваемыми данными. Но, помимо требований внутренней безопасности, серьезной задачей при эксплуатации системы стала разработка защиты ЦОД от внешних атак с учетом требований: стабильность канала до серверов центра; безопасность серверов от внешних проникновений посторонних лиц, защита от проникновения в данные, являющиеся коммерческой тайной компании; устойчивость серверов ЦОД к внешним сетевым атакам; устойчивость ПО центра к вредоносным программам; возможность быстрого восстановления серверов в случае сбоев.

Для реализации защиты сервисов такого ЦОД, сохраняющей компромисс между быстродействием системы, эффективностью и гибкостью защиты, предлагается использовать технологию паравиртуализации приложений. В случае использования ОС от Microsoft данная технология может основываться на технологии Microsoft Hyper-V.

Проведенный в работе анализ и моделирование с использованием диаграмм языка программирования UML формализует задачу и дает достаточно материала для дальнейшего построения математический модели системы защиты, исследования и компьютерного моделирования более надежной изоляции защищаемой сети посредством виртуализации.

Библиографический список

1. *Рыбалко А.А.* Виртуализация как основа систем компьютерной безопасности нового поколения // Вестник МАИ. 2009. Т. 16. № 2. С. 12-18.

2. *Лозовюк А.* Заоблачные вычисления: Cloud Computing на пальцах // Журнал от компьютерных хулиганов «Хакер». 2009. №125. С. 22-25.

3. *Рыбалко А.А.* Технологии виртуализации в фокусе задач компьютерной безопасности // Материалы VII Международной конференции по неравновесным процессам в соплах и струях (NPNJ'2008), 24-31 мая 2008 г., Алушта. М.: Изд-во МАИ, 2008. С. 350-352.

4. *Рыбалко А.А.* Управление виртуальной инфраструктурой, автоматизация средств обеспечения надежности и безопасности серверов внешнего периметра. Технологии Microsoft в теории и практике программирования // Тр. VI Всерос. конф. студентов, аспирантов и молодых ученых. Центральный регион. Москва, 1-2 апреля 2009 г. М.: Вузовская книга, 2009.

5. *Рыбалко А.А.* Виртуализация серверов внешнего периметра в модели защиты корпоративной сети // Материалы XVI Международной конференции по механике и современным прикладным программным системам (ВМСППС'2009), 25-31 мая 2009 г., Алушта. М.: Изд-во МАИ-ПРИНТ, 2009. С. 614-616.

6. www.microsoft.com

7. www.doubletake.com

8. www.quarta.ru

Московский авиационный институт

Статья поступила в редакцию 16.11.2009