I.V. Mashkina, L.R. Tuliganova, I.A. Pavlova

The Development of Detailed Threats Model Applicable for Information Risk Assessment of Enterprise Information System Virtualization Claster

Key words: threat model, virtualization technology, cognitive map

This research on the development of the model object protection – virtual segment industrial enterprises and the development of threat models, with particular attention paid to assisted virtualization hypervisor type I – full virtualization using the system software, working directly with the hardware.

И.В. Машкина, Л.Р. Тулиганова, И.А. Павлова

РАЗРАБОТКА ДЕТАЛИЗИРОВАННОЙ МОДЕЛИ УГРОЗ, ПРИМЕНИМОЙ ДЛЯ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ В СЕГМЕНТЕ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

В течение десяти последних лет в России и на мировом рынке стали активно использоваться решения для реализации технологии виртуализации. Технология виртуализации является эффективным инструментом любого предприятия, позволяющим повысить доступность информации, обеспечить непрерывность бизнес процессов, сэкономить ресурсные вложения по сравнению с физическим резервированием оборудования. Идея заключается в консолидации нагрузок для более эффективного использования серверных ресурсов. В результате применения технологии виртуализации можно достичь: снижения расходов на оборудование, площади и другие ресурсы, простоты восстановления при сбоях, упрощения решения задач масштабирования и администрирования. Поэтому многие предприятия внедряют эту технологию в свои информационные системы (ИС).

Однако использование технологии виртуализации приводит к появлению новых проблем, связанных с обеспечением информационной безопасности (ИБ) как виртуальной среды, так и защищенности ИС предприятия в целом. Для собственника и пользователя информации складывается ситуация, при которой сокрыта истинная реализация используемой системы. В то же время собственник информации должен учитывать риски использования механизмов виртуализации. Риски, связанные с виртуализацией, необходимо оценивать при создании комплексной системы обеспечения информационной безопасности (СОИБ) предприятия и при проведении внутреннего аудита. При оценке рисков нарушения ИБ в виртуальных средах необходимо учитывать ряд особенностей: реализуя атаку из среды гипервизора, злоумышленник имеет возможность нарушить целостность и конфиденциальность данных на дисках виртуальных машин (ВМ) даже, если они не работают. Под ВМ понимается программная система, эмулирующая аппаратное обеспечение некоторой платформы. Кроме того, наличие уязвимостей компонентов виртуальной инфраструктуры может привести к нарушению изоляции гостевых операционных систем и экземпляров ВМ друг от друга при обработке на одном физическом сервере информации с различными метками бизнес категоризации и разного уровня критичности, что также повышает риски нарушения ИБ.

Таким образом, существует необходимость предотвращения несанкционированного доступа и контроля административных ролей в виртуальной среде.

Для решения проблемы обеспечения защищенности ИС предприятия с учетом *приведенных выше особенностей* виртуальной среды необходимо, в первую очередь, провести следующие исследования: разработать модель объекта защиты – виртуального сегмента ИС предприятия – и разработать модель угроз нарушения ИБ, что позволит, используя существующие в настоящее время решения, сделать обоснованный выбор средств и механизмов защиты, оценить риски использования технологии виртуализации.

Требования, касающиеся защиты виртуальных инфраструктур, содержатся в нормативных документах: приказах №17, №21 ФСТЭК [1, 2]. Специалисты в области ИБ многих стран следуют рекомендациям международного стандарта NISTP800-125 [3], на основе которого можно разработать политику безопасности в виртуальной среде; в документе приводятся рекомендации по защите гипервизора и гостевых ОС.

Разработан проект ГОСТ-Р: «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации, основные положения» [4]. В соответствии с этим документом защите подлежат: физические и виртуальные диски с образами ВМ, системное и прикладное программное обеспечение, в том числе гипервизоры I и II типов, данные и резервные копии данных, сетевое оборудование, конфигурационные файлы.

Защита информации в любой информационной системе, в том числе построенной на основе использования технологии виртуализации, – это деятельность, заключающаяся в создании барьеров, назначение которых обеспечивать защиту данных от доступа неавторизованного субъекта. Поскольку *барьеры* призваны обеспечивать безопасность на путях распространения потенциально возможных угроз, для определения мест размещения средств защиты в ИС предприятия, функционирующей с использованием технологии виртуализации, должна быть построена детализированная модель угроз нарушения безопасности *виртуальной среды*.

На основе этих документов и предыдущих исследований авторов [5] разработана структурная вербальная модель сегмента виртуализации и детализированная модель угроз нарушения безопасности в виртуальной среде в виде нечеткой когнитивной карты.

Для построения модели угроз необходимы исходные данные об ИС предприятия: сведения о топологии локальной или корпоративной вычислительной сети, о числе локальных сетевых сегментов, количестве компьютеров, об инфраструктуре и применяемом решении виртуализации, сведения о подразделениях предприятия, сотрудники которых авторизованы для работы в виртуальной среде, информация о том, имеются ли точки доступа в глобальную сеть Интернет.

Модель угроз согласуется с политикой безопасности предприятия, в основе формирования которой – требования реализации бизнес-процессов. При построении модели угроз в информационной системе предприятия, функционирующей с использованием технологии виртуализации, необходимы сведения о *конкретном объекте защиты* для того, чтобы учесть все возможные пути реализации угроз, осуществляемых на стороне пользователя виртуального сегмента и в сети: угроз на уровне физической инфраструктуры и на уровне виртуальной среды.

Возможный вариант архитектуры ИС с сегментом виртуализации приведен на рис. 1 для случая, когда сеть не имеет доступа в Интернет. В этом случае работа в клиент-серверном варианте возможна напрямую с кластером виртуализации.

Сеть базируется на коммутаторах CiscoCatalyst. Клиент – серверная архитектура разделяет всю функционирующую ИС на три различные части, определенным образом взаимодействующие между собой: клиентское приложение, сеть, кластер серверов вир-

туализации. При выполнении даже сложных запросов программа, работающая у пользователя, получает необходимую выборку, а преобразование данных осуществляется на кластере серверов виртуализации. Трехуровневая архитектура обеспечивает упорядочивание доступа пользователей к информации и предоставляет удобство администрирования. При обращении к той или иной базе данных пользователь должен указать кластер и имя информационной базы. Он работает с удобным для себя представлением объекта через виртуальную машину, для него не имеет значения, какова структура объекта.

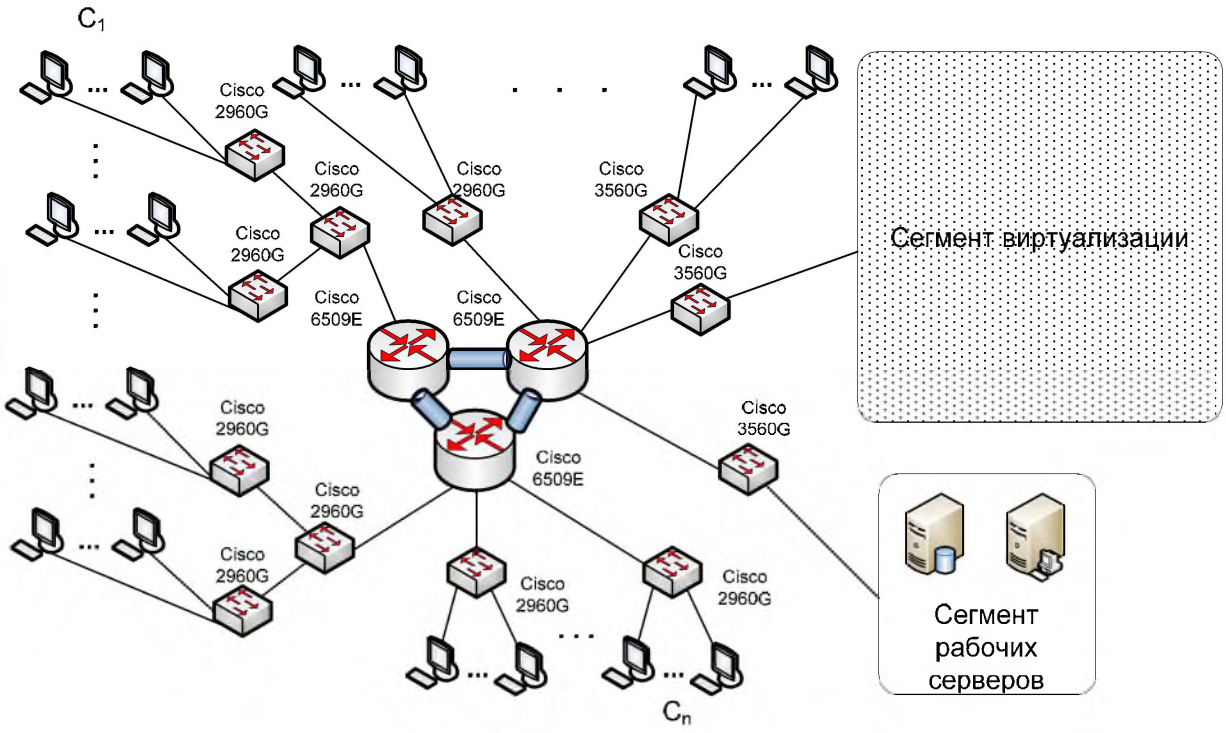

Рис. 1. Топология сети предприятия

Таким образом, обращение пользователя – сотрудника какого-либо подразделения предприятия к сегменту виртуализации может происходить по схеме «тонкий» клиент, который взаимодействует с файловой базой данных, хранящейся на физическом сервере StorageSystem. При работе «тонкого» клиента организуется специализированная среда, в рамках которой загружаются необходимые для работы компоненты серверной системы и прикладная конфигурация, выполняются действия и процессы, необходимые для нормальной работы системы с информационной базой.

Рассмотрим сегмент виртуализации сети предприятия, приведенный на рис. 2, базирующийся на продукте VMWare, который основан на виртуализации серверных ОС.

Администратор виртуализации поддерживает работу гипервизора ВМ и других компонентов виртуализации через управляющий компонент, предоставляющий администратору анализ состояния конфигурации кластеров, виртуальных машин, хранилища, хостовых и гостевых ОС в единой консоли. При этом производительность работы администратора виртуализации почти в два раза превышает производительность управления физической инфраструктурой, предназначенной для того же объема работы.

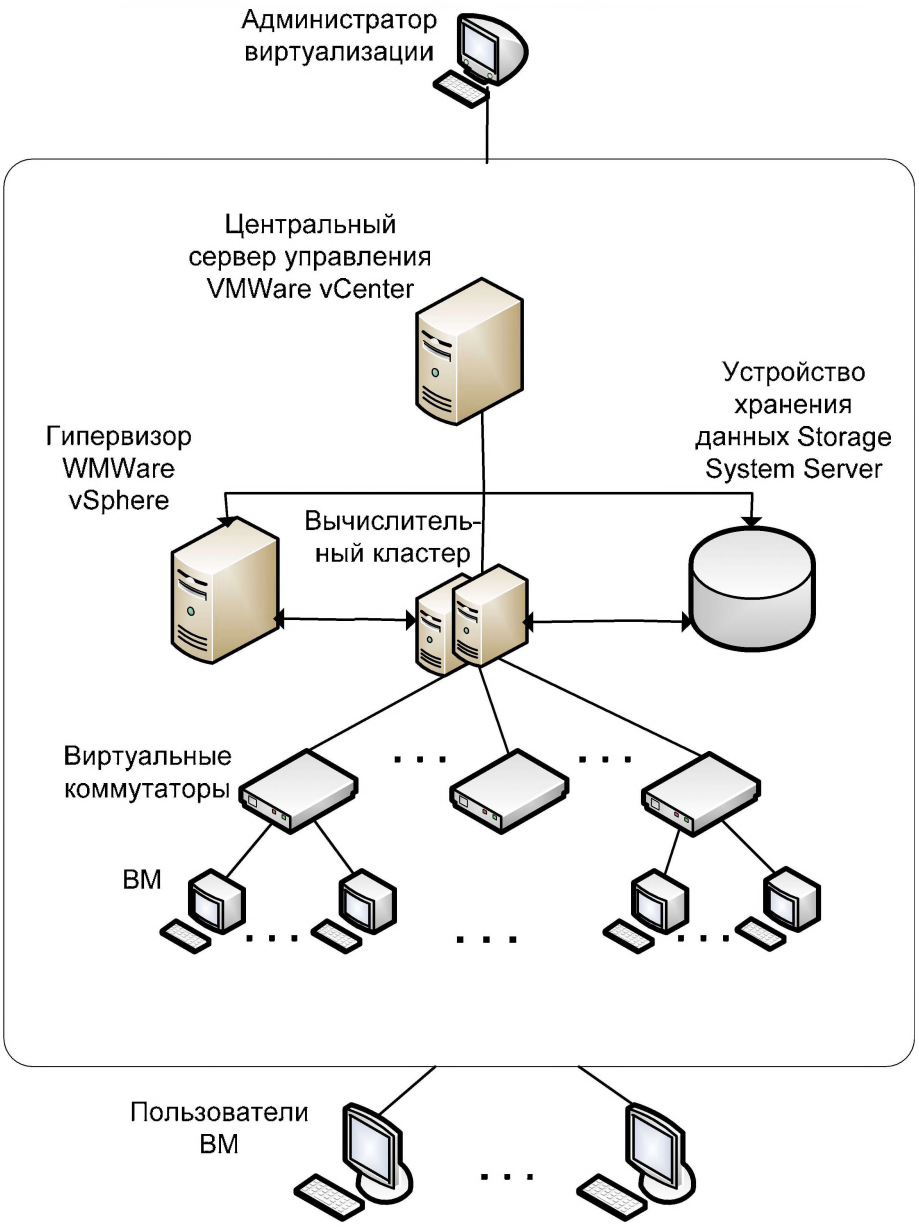

Рис. 2. Сегмент виртуализации сети предприятия

В [5] авторами был предложен формат структурной вербальной модели объекта защиты, функционирующего с использованием технологии виртуализации *в общем виде*. В данной работе конкретное наполнение формата модели выполняется для варианта ИС, архитектура которой приведена на рис. 1 и 2. При разработке модели объекта защиты необходимо включить в нее не только оборудование и технологии сегмента виртуализации, но и клиентские составляющие для работы с сегментом виртуализации.

Модель, представленная в табл.1, отображает в организованном структурированном виде информацию о сегменте виртуализации, об особенностях используемой технологии виртуализации.

Таблица 1. Модель объекта защиты

№ п.п.	Тип ресурса				
1	Средства вычислительной техники				
1	2	3	4	5	6
№ элемента ресурса	Наименование элемента ресурса	Уровень физического доступа	Поддерживаемые LAN-протоколы	Встроенные сервисы безопасности	Месторасположение элемента ресурса
1.1	Терминалы пользователей виртуальных машин	Сотрудники соответствующего отдела предприятия	Ethernet, стек протоколов TCP/IP	Антивирус (АВ) и др.	Соответствующие отделы предприятия
1.2	Рабочая станция администратора виртуализации	Администратор виртуализации	Ethernet, стек протоколов TCP/IP	Active Directory (AD), АВ	Административный сегмент
1.3	Рабочая станция администратора безопасности	Администратор безопасности		AD, АВ	Административный сегмент
1.4	Физические серверы с запущенными виртуальными машинами (экземплярами)	Администратор безопасности, администратор виртуализации		Access Control List (ACL), AD, АВ	Серверная кластера виртуализации ИС
1.5	Физический сервер хранения данных (Storagesystemserver)	Администратор безопасности, администратор виртуализации		ACL, AD, АВ	Серверная кластера виртуализации ИС
2	Информационные технологии				
№ элемента ресурса	Наименование элемента ресурса	Уязвимости соответствующих программ	Уровень критичности	Ценность элемента ресурса	Субъект доступа	Месторасположение элемента ресурса
1	2	3	4	5	6	7
2.1 Системное ПО						
2.1.1	Гипервизор I типа vSphere ESXi	CVE-2013-1405, CVE-2012-5703, CVE-2012-1666, CVE-2011-1789	Высокий		Администратор виртуализации	Сервер VMWare

Продолжение табл. 1

1	2	3	4	5	6	7
2.1.2	ГостеваяОС Windows 7 Professional SP1	CVE-2010-4182			Администратор виртуализации, клиент ВМ	Сервер VMWare
2.1.3	Консоль vSphere Client	CVE-2014-1210, CVE-2014-1209, CVE-2013-1405, CVE-2013-5971, CVE-2012-1512.			Администратор виртуализации, клиент ВМ	Рабочая станция администратора виртуализации, терминалы клиентов ВМ
2.2 Прикладное ПО						
2.2.1	Платформа управления виртуализации (VMWarevCenterServer)	CVE-2014-3790, CVE-2013-5973, CVE-2013-1212, CVE-2013-3107			Администратор виртуализации	ПК администратора виртуализации
2.2.2	Виртуальные машины (образы узлов vSphere)	CVE-2014-3790, CVE-2014-1210, CVE-2014-1209, CVE-2013-5556			Администратор виртуализации, клиента ВМ	Сервер VMWare (библиотека AutoDeploy)
2.2.3	Active Directory	CVE-2014-8764, CVE-2014-0602			Администратор безопасности	Сервер VMWareESX
2.2.4	Службы, сервисы, драйверы VMWare	CVE-2014-3608, CVE-2014-6278, CVE-2014-7187, CVE-2014-7169			Администратор виртуализации, клиенты ВМ	Сегмент виртуализации
2.3 Виртуальные средства безопасности						
2.3.1	Виртуальный межсетевой экран Virtual Firewall/VPN	CVE-2013-6398, CVE-2007-4967, CVE-2006-7160			Администратор виртуализации	Периметр виртуальной инфраструктуры
2.3.1	Виртуальная система обнаружения вторжений Virtual IPS	CVE-2010-0827				

3	Информационные ресурсы			
№ элемента ресурса	Наименование элемента ресурса	Уровень критичности	Субъект доступа	Расположение ресурса
1	2	3	4	5
3.1	Базы данных		Сотрудники-пользователи виртуальных машин	Томана Storage System Server

Окончание табл. 1

1	2	3	4	5
3.2	Файлы образов и снимков виртуальных машин		Сотрудники-пользователи виртуальных машин, администратор виртуализации	Хранилищеданных SAN/Storage System Server
3.3	Служебная информация		Администратор виртуализации, администратор безопасности	Рабочая станция администратора виртуализации, администратора безопасности
3.4	Резервные копии данных физического и виртуального пространства		Администратор виртуализации	Хранилищеданных SAN/Storage System Server
3.5	Файлы параметров конфигурации		Администратор безопасности	Выделенный сервер, рабочая станция администратора безопасности
3.6	Служебная информация виртуальных устройств		Сотрудники-пользователи виртуальных машин	Рабочая станция пользователя

4	Аппаратура, каналы и линии связи (примеры)			
№ элемента ресурса	Наименование элемента ресурса	Реализуемая технология	Пропускная способность	Встроенные сервисы безопасности
4.1	Маршрутизаторы			
4.2	Коммутаторы 3 уровня, 2 уровня			
4.3	Виртуальные коммутаторы (CiscoNexus 1000v)			
4.4	Одномодовый оптический кабель(LX)			
4.5	Медная витая пара категории 5 (TX)			

В таблице в столбце «уязвимости соответствующих программ» приведены обозначения уязвимостей из [6]. Например, уязвимость CVE-2013-6398 позволяет удаленному пользователю обойти ограничения настроек, CVE-2014-1309 дает возможность загрузки произвольной команды.

Различные решения, реализующие технологию виртуализации, имеют встроенные в платформу сервисы безопасности, позволяющие специалистам отдела безопасности применять политики безопасности для приложений. Так, в системе VMWare модуль VMWarevShieldZones поддерживает сегментацию сети для пользователей и конфиденциальных данных, обеспечивает безопасность приложений за счет применения корпоративных политик безопасности в общей виртуальной среде на уровне приложений.

Часто механизм аутентификации реализуется в сети через службу ActiveDirectory (AD). Для удобного и быстрого управления политиками безопасности на виртуальных томах они должны быть введены в домен AD.

Если на гипервизор реализуется успешная атака, то нарушитель получит возможность доступа к образам ВМ на StorageSystemServer, что позволит ему читать и изменять данные на дисках. Кроме того, осуществив успешную атаку на гипервизор, нарушитель сможет получить доступ к работающему экземпляру и копировать поток данных на такие устройства, как: принтер, USB, HDD.

Известно, что все распространенные в настоящее время криптографические алгоритмы не позволяют производить вычисления над зашифрованными данными без предварительной расшифровки [7]. Поэтому возможность реализации определенной части угроз в виртуальной среде связана с тем, что вычисления на экземплярах ВМ выполняются в незашифрованном виде. Атаки на образы виртуальных машин, которые хранятся на сервере хранения данных StorageSystemServer, возможны при наличии уязвимостей МСЭ и системы разграничения доступа к дискам ВМ. Атаки, указанные выше, могут быть реализованы, если нарушитель получит доступ к средствам администрирования. Важное значение имеет правильность настроек средств управления физической и виртуальной инфраструктурой, использование виртуальных средств защиты, контролирующих трафик внутри сервера виртуализации. Централизованный процесс управления ВМ должен соответствовать политике безопасности предприятия.

На основе структурной вербальной модели объекта защиты и технологии моделирования угроз [8] разработана *детальная* графовая модель в виде нечеткой когнитивной карты. При этом рассматриваются угрозы, которые приводят к перехвату управления в среде виртуализации, реализуемые за счет: атак на гипервизор и виртуальные каналы передачи, нарушения процедур аутентификации субъектов доступа в виртуальной среде, нарушения изоляции ВМ, несанкционированного доступа к образам ВМ и средствам виртуализации, – со стороны пользователей физической сети предприятия, пользователей виртуального сегмента, работающих с экземплярами ВМ как на одном и том же физическом сервере, что и атакуемая ВМ, так и на разных физических серверах. Детализированная модель угроз нарушения ИБ в сегменте виртуализации ИС предприятия приведена на рис.3.

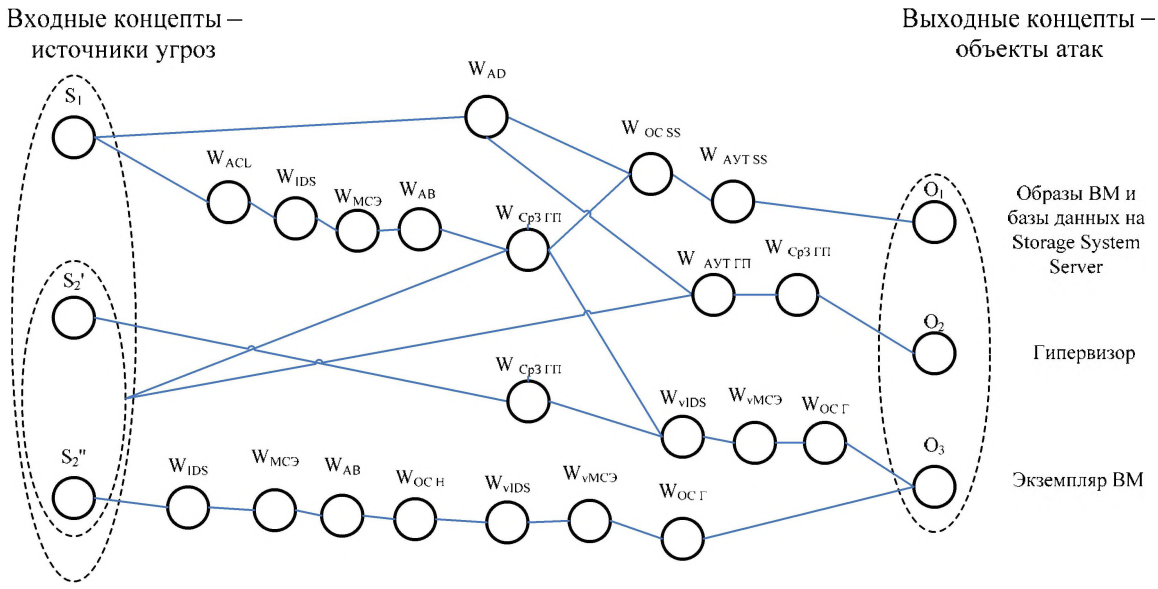

Рис. 3. Нечеткая когнитивная карта – модель угроз

При построении нечеткой когнитивной карты (НКК) в рассмотрение принимались следующие уязвимости: ошибки в разработке политики безопасности, когда есть неограниченный административный доступ к интерфейсам управления гипервизором, не отключенные от хост системы, неиспользуемые физические и аппаратные средства, не отключенные ненужные службы гипервизора, отсутствие контроля безопасности каждой гостевой ОС, неустановленные обновления гипервизора, неустановленное обновление гостевых ОС, не отключенные неиспользуемые аппаратные средства для каждой гостевой ОС, отсутствие защиты хостовых ОС.

При построении когнитивной карты в качестве входных концептов $S_j (j \in 1,3)$ – источников угроз принимались: S_1 – пользователь физической сети, неавторизованный для работы в ВС, S_2' – сотрудник-пользователь виртуального сегмента, работающий на одном физическом сервере с атакуемой ВМ, S_2'' – сотрудник-пользователь виртуального сегмента, атакующий ВМ, запущенную на другом физическом сервере; в качестве выходных концептов $O_i (i \in 1,3)$ – объекты атак: O_1 – базы данных и образы ВМ на StorageSystemServer, O_2 – системное ПО – гипервизор I типа, O_3 – работающий экземпляр виртуальной машины на сервере вычислительного кластера. Промежуточные концепты – уязвимости аппаратуры связи, физических и виртуальных средств защиты, механизмов защиты, ОС.

НКК построена для следующих исходов реализации угроз: получение контроля над StorageSystemServer, получение контроля над гипервизором, получение контроля над экземпляром.

Вероятность реализации угрозы одному *i*-му объекту от одного источника угрозы может быть вычислена по формуле:

$$P_i = P_{\text{акт}} \cdot \max(P_{y1} \cdot P_{y2} \cdot \ldots \cdot P_{yk}), \quad (1)$$

где k – число промежуточных концептов на пути атаки,

$P_{\text{акт}}$ – вероятность активизации источника угрозы,

P_i – вероятность угрозы на *i*-м пути от источника к объекту атаки,

P_y – вероятность уязвимости.

Вероятность реализации угрозы объектам O_1, O_2 от возможных двух источников угроз могут быть вычислены по формуле:

$$P_i^U = 1 - \prod_{i=1}^{2} (1 - P_i), \quad (2)$$

Вероятность реализации угрозы объекту O_3 от возможных трех источников угроз может быть вычислена по формуле:

$$P_i^U = 1 - \prod_{i=1}^{3} (1 - P_i), \quad (3)$$

Величина относительного риска вычисляется по формуле:

$$\overline{R} = \sum_{i=1}^{I} P_i^U \cdot \overline{\text{Ц}}_i, \quad (4)$$

где I – число информационных объектов,

Ц_i – численное значение ценности ресурса.

На основе модели угроз в виде НКК проведены расчеты значений уровней угроз и сделана количественная оценка уровня риска нарушения безопасности сегмента виртуализации при использовании технологии виртуализации, базирующейся на WMWare в качестве примера. Численные значения уязвимостей компонентов инфраструктуры и

сервисов безопасности приведены в [6], в расчетах используются их нормированные значения.

Таким образом, предложенная детализированная модель угроз нарушения ИБ сегмента виртуализации в виде нечеткой когнитивной карты позволяет визуализировать возможные пути реализации угроз и применима в задачах управления рисками в виртуальных средах.

Работа выполнена при поддержке гранта РФФИ № НЧ-НЧ-05-14-ГФ.

СПИСОК ЛИТЕРАТУРЫ:

1. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». URL: http:// www.ib.ru/law/3178 (Дата обращения 29.10.2014).
2. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».URL: http://www.ib.ru/law/3177 (Датаобращения 29.10.2014).
3. National Institute of Standards and Technology. Special Publication 800-125. Guide to Security for Full Virtualization Technologies. *URL:*http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf (Дата обращения 29.10.2014).
4. ГОСТ Р XXXXX – 20XX (проект, первая редакция). Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения. URL: https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVln (Дата обращения 29.10.2014).
5. Тулиганова Л.Р., Павлова И.А., Машкина И.В. Разработка моделей объекта защиты и угроз нарушения безопасности в информационной системе, базирующейся на технологии виртуализации // Известия ЮФУ. Технические науки № 8 (157) – Таганрог: Изд-во ТТИ ЮФУ, 2014. – С. 32-41.
6. National Vulnerability Database. URL: http://nvd.nist.gov/ (датаобращения 29.10.2014).
7. Жиров А.О., Жирова О.В., Кренделев С.Ф. Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий.– 2013. – №1. С. 6-12.
8. Гузаиров М.Б., Машкина И.В., Степанова Е.С.Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. – 2011. – №2. С. 37-49.

REFERENCES:

1. Prikaz FSTEK Rossii ot 11.02.2013 N 17 «Ob utverzhdenii trebovanij o zaschite informatsii, ne sostavlyayushej gosudarstvennuyu tajnu, soderzhashejsya v gosudarstvennyh informatsionnyh sistemah». URL: http:// www.ib.ru/law/3178 (Data obrashcheniya 29.10.2014).
2. Prikaz FSTEK Rossii ot 18.02.2013 N 21 «Ob utverzhdenii sostsva i soderzhaniya organizatsionnyh mer po obespecheniyu bezopasnosti personalnyh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh». URL: http://www.ib.ru/law/3177 (Data obrashcheniya 29.10.2014).
3. National Institute of Standards and Technology. Special Publication 800-125.
Guide to Security for Full Virtualization Technologies. URL: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf (Data obrashcheniya 29.10.2014).
4. GOST R XXXXX – 20XX (proekt, pervaya redaktsiya). Zashchita informatsii. Trebovaniya po zashchite informatsii, obrabatyvaemoj s ispolzovaniem tehnologii virtualizatsii. Obshie polozheniya.
URL: https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVln (Data obrashcheniya 29.10.2014).
5. Tuliganova L.R., Pavlova I.A., Mashkina I.V. Razrabotka modelej ob'ekta zashchity i ugroz narusheniya bezopasnosti v informatsionnoi sisteme, bazirueshcheisya na tekhnologii virtualizatsii // Izvestiya YUFU. Tekhnicheskie nauki № 8 (157) – Taganrog: Izd-vo TTI YUFU, 2014. – S. 32-41.
6. National Vulnerability Database. URL: http://nvd.nist.gov/ (Data obrashcheniya 29.10.2014).
7. Zhirov A.O., Zhirova O.V., Krendelev C.F. Bezopasnye oblachnye vychisleniya s pomoshch'yu gomomorfnoi kriptografii // Bezopasnost' informatsionnyh tekhnologii. – 2013. – №1. S. 6-12.
8. GuzairovM.B., MashkinaI.V., StepanovaE.S. Postroeniemodeliugrozspomoshch'yunechetkikhkognitivnykhkartnaosnovesetevoipolitikibezopasnosti // Bezopasnost' informatsionnyhtekhnologii. – 2011. №2. S. 37-49.