УДК 004.9

К.В. Курносов, В.В. Селифанов

Разработка требований для оценки безопасности виртуальной инфраструктуры

В соответствии с руководящими и методическими документами в области технической защиты информации была разработана модель инфраструктуры, построенной с применением технологии виртуализации, в которой содержится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну. Были определены виды потенциальных нарушителей безопасности, выделены актуальные угрозы и выработан набор требований для оценки безопасности таких инфраструктур.

Ключевые слова: виртуализация, виртуальная инфраструктура, виртуальная машина, гипервизор, информационная безопасность, требования информационной безопасности.

Обзор технологии виртуализации. Специфика современного рынка производства и услуг приводит к необходимости обработки огромных информационных потоков в реальном времени с повышенными требованиями к безопасности и надежности. Для продуктивной работы организаций требуется все больше и больше сервисов, предоставляемых как для клиентов, так и для собственных сотрудников. Запуск большого количества разнообразных служб и приложений на одном сервере ведет к увеличению финансовых потерь и иного ущерба, в случае выхода его из строя или реализации других возможных угроз.

Для обеспечения минимизации таких рисков очевидным представляется решение использовать для каждого сервиса отдельно выделенный сервер. Это делается в первую очередь для изоляции приложений друг от друга. Такой подход приводит к быстрому росту самих серверов, локальных сетей и инженерных коммуникаций. Следствием этого непременно становится неконтролируемый рост расходов на содержание информационной инфраструктуры, а также сложности с ее управлением и масштабируемостью.

Виртуализация является одной из ключевых технологий, позволяющих решить большинство этих проблем и перейти от экстенсивного развития инфраструктуры к интенсивному.

В проекте ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» [1. С. 2] под виртуализацией понимают создание программных систем на основе существующих аппаратно-программных комплексов, зависящих или не зависящих от них. Под виртуальной инфраструктурой (ВИ), в том же документе [1. С. 4], подразумевается сформированная совокупность физических компьютеров и серверов, виртуальных ресурсов и компонентов виртуальной платформы (ВП), развернутых на физических серверах, а также каналы связи.

Данная технология несет такие преимущества, как оптимальное использование вычислительных ресурсов, экономия ресурсов материальных, повышение возможностей масштабирования инфраструктуры и увеличение уровня отказоустойчивости.

Конечно, как и все технологии, технология виртуализации не совершенна и обладает своими недостатками. Технологии виртуализации порождают новые специфические угрозы. Примерами таковых могут являться угрозы гипервизору, угрозы образам виртуальной машины (ВМ) и виртуальным сетевым инфраструктурам.

Согласно статистике «Лаборатории Касперского» [2] 59% опрошенных российских компаний с локальными сетями от 100 компьютеров и выше уже внедрили или планируют внедрить виртуализацию серверов.

По данным исследований Cisco Systems, Inc [3], в качестве основных препятствий для использования технологий виртуализации в своих информационных системах (ИС) крупные компании чаще других упоминают вопросы безопасности (23% случаев). Таким образом, можно сделать вывод, что вопросы виртуализации и обеспечения ее безопасности на сегодняшний день довольно актуальны как в России, так и в мире в целом.

Анализ существующих информационных технологий реализующих ВИ показал, что для обеспечения их безопасности необходимо построение систем защиты информации, способных устранять специфичные угрозы, возникающие при использовании технологий виртуализации.

Постановка задачи. Ввиду отсутствия требований для технологий, реализующих ВИ, была поставлена цель по их разработке в соответствии с действующими в этой сфере нормативными и методическими документами. Для достижения поставленной цели необходимо было решить ряд задач. Во-первых, разработать модель ВИ, для которой будет строиться система защиты. Во-вторых, определить потенциальных нарушителей безопасности и выделить актуальные угрозы. В-третьих, проанализировать требования регуляторов, предъявляемые к системам, в которых могут быть использованы технологии виртуализации.

Модель виртуальной инфраструктуры. В случае если среда виртуализации используется для построения ИС, в которых содержится информация ограниченного доступа, то необходимо чтобы средства защиты информации прошли процедуру оценки соответствия. Документы, в которых определены меры по защите среды виртуализации, – проект ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» [1. С. 14–28] и Приказы ФСТЭК России №17 [6. С. 19] и №21 [7. С. 6].

На основе указанных выше документов, описания архитектуры и выделенных объектов защиты, при использовании технологии виртуализации, существующих в этих документах, была разработана модель ВИ, включающая ее основные компоненты (рис. 1).

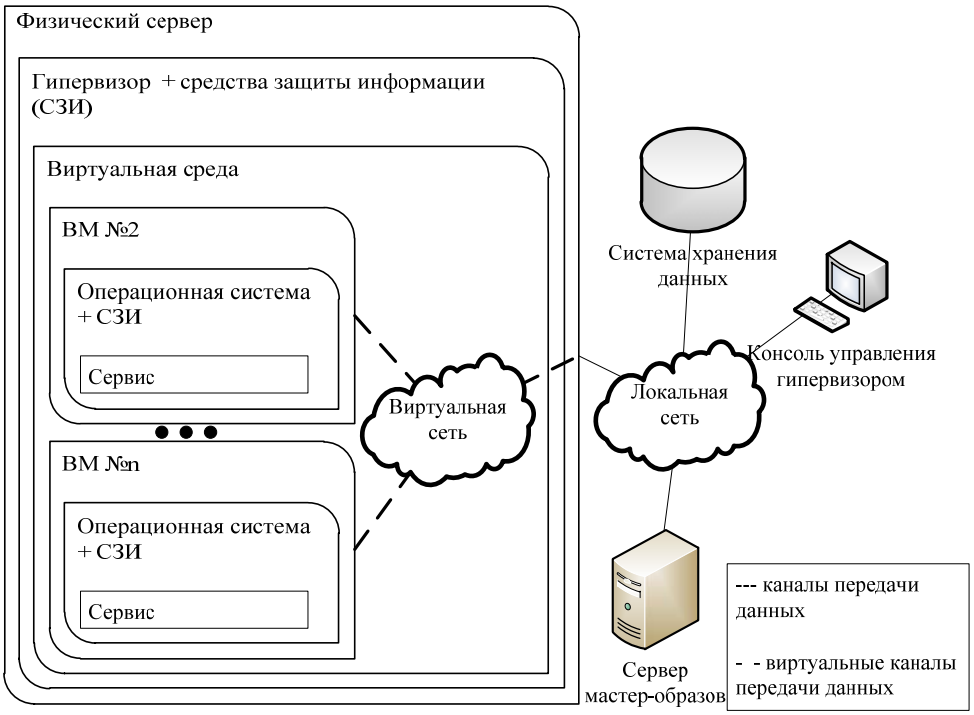

Рис. 1. Модель виртуальной инфраструктуры

Нарушитель и угрозы безопасности виртуальной инфраструктуры. Для определения угроз безопасности информации и разработки модели угроз в рамках данной статьи была разработана модель нарушителя безопасности ВИ.

В соответствии с методиками ФСТЭК России и ФСБ России [4, 5] все нарушители были поделены на внутренних и внешних. Внешние нарушители подразделяются на 2 категории: категория I (лица, не имеющие права доступа в контролируемую зону информационной системы) и категория II (лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы). К внешним нарушителям I категории относятся: бывшие сотрудники предприятия и посторонние лица, действующие в инициативном порядке. К внешним нарушителям II категории относятся представители преступных организаций. К внутренним нарушителям относятся: сотрудники организации, с разными правами доступа к компонентам системы, персонал, не имеющий легитимного доступа к компонентам системы, и лица из сторонних организаций, имеющие прямой или косвенный доступ к компонентам инфраструктуры.

Для каждого нарушителя были выделены возможные объекты атаки, средства атаки и используемые ими уязвимости. Общий перечень угроз, характерных для ВИ, приведен в проекте ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»[1. С. 7–13].

Требования для оценки безопасности виртуальной инфраструктуры. Отталкиваясь от данных угроз и модели нарушителя, были разработаны требования безопасности для ВИ, являющихся частью ИС, в которых не ведется обработка сведений, составляющих государственную тайну. В соответствии с Приказом ФСТЭК России №17 [6. С. 6] устанавливаются четыре класса защищенности ИС, в том числе и ИС, реализованных на базе ВИ. Классы защищенности ранжируются по возрастанию требований от четвертого до первого. Ниже представлена таблица, в которой сведены воедино классы защищенности и требования, предъявляемые к ним.

Требования безопасности для ВИ, являющихся частью ИС

№	Требования	Класс защищенности			
		4	3	2	1
Т1	Требования к идентификации и аутентификации субъектов доступа и объектов доступа в ВИ, в том числе администраторов	+	+	++	++
Т2	Требования к управлению доступом субъектов доступа к объектам доступа в ВИ, в том числе внутри ВМ	+	++	++	++
Т3	Требования к регистрации событий безопасности в ВИ	–	+	+	+
Т4	Требования к управлению (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами ВИ, а также по периметру ВИ	–	–	+	++
Т5	Требования к доверенной загрузке серверов виртуализации (гипервизор), ВМ, серверов управления виртуализацией (консоль управления гипервизором)	–	–	–	–
Т6	Требования к управлению перемещением ВМ и обрабатываемых на них данных	–	–	+	++
Т7	Требования к контролю целостности ВИ и ее конфигураций	–	–	+	+
Т8	Требования к резервному копированию данных, резервированию технических средств, программного обеспечения ВИ, а также каналов связи внутри ВИ	–	–	+	++
Т9	Требования к реализации и управлению антивирусной защитой в ВИ	–	+	++	++
Т10	Требования к разбиению ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей	–	–	+	++
Т11	Минимальный требуемый класс СВТ при построении ИС	5	5	5	5
Т12	Минимальный требуемый класс СОВ при построении ИС (в случае взаимодействия с сетями международного обмена)	5	5(4)	4	4
Т13	Минимальный требуемый класс МЭ при построении ИС (в случае взаимодействия с сетями международного обмена)	4	4(3)	4(3)	4(3)
Т14	Минимальный требуемый класс антивирусной защиты, при построении. ИС (в случае взаимодействия с сетями международного обмена)	5	5(4)	4	4
Т15	Минимальный требуемый уровень контроля отсутствия НДВ для используемого в ИС программного обеспечения	–	–	4	4

*+ требование предъявляется; ++ предъявляются усиленные требования; – требования не предъявляются.

В данной статье был сделан акцент на разборе требований, предъявляемых к системам защиты информации, разработанным для ВИ, построенных в соответствии с I классом защищенности как наиболее полном.

Т1. Требования к идентификации и аутентификации субъектов доступа и объектов доступа в ВИ, в том числе администраторов.

Идентификация и аутентификация субъектов и объектов доступа должна осуществляться в соответствии с требованиями ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7 из методического документа ФСТЭК России «Меры защиты информации в государственных информационных системах» [5. С. 16–24].

В качестве объектов доступа в ВИ необходимо рассматривать программное обеспечение управления ВИ, гипервизор, хостовую операционную систему (для гипервизора 2-го типа), ВМ, виртуализированное программное обеспечение, СЗИ, используемые в рамках ВИ.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в ВИ должны обеспечиваться:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в ВИ;

– блокировка доступа к компонентам ВИ для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации в процессе ее ввода для аутентификации в ВИ от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления аппаратного обеспечения ВИ.

Внутри развернутых ВМ должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1–ИАФ.7 [5. С. 16–24].

Требования усиления. В ИС должны обеспечиваться взаимная идентификация и аутентификация пользователя и ВМ при удалённом доступе.

Т2. Требования к управлению доступом субъектов доступа к объектам доступа в ВИ, в том числе внутри ВИ.

Эту функцию в части управления доступом к ВИ выполняет гипервизор или СЗИ. Но управление доступа внутри ВМ эти средства выполнить не могут, в этом случае используются классические СЗИ от НСД, устанавливаемые на ВМ.

В ВИ должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри ВМ, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13 из [Там же. С. 25–41].

При реализации мер по управлению доступом субъектов доступа к объектам доступа в ВИ должны обеспечиваться:

– контроль доступа субъектов доступа к средствам управления компонентами ВИ;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, ВМ, файлам-образам ВМ;

– управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

– контроль запуска ВМ на основе заданных оператором правил;

– разграничение доступа субъектов доступа, зарегистрированных на ВМ, к объектам доступа, расположенным внутри ВМ, в соответствии с правилами разграничения доступа пользователей данных ВМ;

– разграничение доступа субъектов доступа, зарегистрированных на ВМ, к ресурсам ВИ, размещенным за пределами ВМ, в соответствии с правилами разграничения доступа.

Требования усиления. В ВИ должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления ВМ, в том числе к операциям создания, запуска, останова, создания копий, удаления ВМ, который должен быть разрешен только администраторам ВИ.

Т3. Требования к регистрации событий безопасности в ВИ.

Должна обеспечиваться регистрация событий безопасности в соответствии с РСБ.1, РСБ.2, РСБ.3, РСБ.4 и РСБ.5 [Там же. С. 62–69].

При реализации мер по регистрации событий безопасности в ВИ дополнительно к событиям, установленным в РСБ.1 [Там же. С. 62], должны подлежать регистрации: запуск и завершение работы компонентов ВИ, доступ субъектов доступа к компонентам ВИ, изменения в составе и конфигурации компонентов ВИ во время их запуска, функционирования и аппаратного отключения.

Для данных событий должны быть зафиксированы: дата и время события, результат события (успешный или неуспешный), идентификатор пользователя, инициировавшего событие.

Т4. Требования к управлению потоками информации между компонентами ВИ, а также по периметру ВИ.

В ИС должно осуществляться управление потоками информации между компонентами ВИ и по периметру ВИ в соответствии с УПД.3, ЗИС.3 [Там же. С. 29–31, 124], при этом должны обеспечиваться:

– фильтрация сетевого трафика между компонентами ВИ, в том числе между внешними и внутренними по отношению к ВМ сетями;

– наличие доверенных маршрутов внутри ВИ между администратором, пользователем и СЗИ (функциями безопасности);

– контроль передачи служебных информационных сообщений по составу и объёму;

– отключение неиспользуемых сетевых протоколов гипервизора, хостовой операционной системы, виртуальной вычислительной сети компонентами ВИ;

– обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри ВИ, в том числе для защиты от подмены сетевых устройств и сервисов;

– обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами ВИ и сетевых потоков виртуальной вычислительной сети;

– семантический и статистический анализ сетевого трафика.

Требования усиления. Должна быть обеспечена единая точка подключения к ВИ. В ИС должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой ВМ.

Т6. Требования к управлению перемещением ВМ и обрабатываемых на них данных.

Оператором должно обеспечиваться управление перемещением ВМ и обрабатываемых на них данных. При этом должны обеспечиваться:

– регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

– управление размещением и перемещением данных, файлов-образов и исполняемых файлов ВМ.

Управление перемещением ВМ должно предусматривать возможность обеспечить:

– полный запрет перемещения ВМ;

– ограничение перемещения ВМ в пределах информационной системы;

– ограничение перемещения ВМ между сегментами ИС.

Требования усиления. Оператором должна осуществляться обработка отказов перемещения ВМ (контейнеров) и обрабатываемых на них данных.

Т7. Требования к контролю целостности ВИ и ее конфигураций.

В ИС должен обеспечиваться контроль целостности компонентов ВИ в соответствии с ОЦЛ.1 [5. С. 86–88]. При реализации мер по контролю целостности компонентов ВИ должны обеспечиваться:

– контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и ВМ;

– контроль целостности файлов-образов виртуализированного программного обеспечения и ВМ, файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

– контроль целостности резервных копий ВМ.

Т8. Требования к резервному копированию данных, резервированию технических средств, программного обеспечения ВИ, а также каналов связи внутри ВИ.

В ИС должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения ВИ и каналов связи внутри ВИ в соответствии с ОДТ.2, ОДТ.4, ОДТ.5 [Там же. С. 96–102]. При реализации этих требований должны обеспечиваться:

– определение мест хранения резервных копий ВМ и данных, обрабатываемых в ВИ;

– резервное копирование ВМ;

– резервное копирование данных, обрабатываемых в ВИ;

– резервирование программного обеспечения ВИ;

– резервирование каналов связи, используемых в ВИ;

– периодическая проверка резервных копий и возможности восстановления ВМ и данных, обрабатываемых в ВИ с использованием резервных копий.

Требования усиления. В ИС должно выполняться резервное копирование конфигурации ВИ, программного обеспечения серверов управления виртуализацией, автоматизированного рабочего

места администратора управления средствами виртуализации, а также дистрибутивов средств построения ВИ.

Т9. Требования к реализации и управлению антивирусной защитой в ВИ.

В ИС должны обеспечиваться реализация и управление антивирусной защитой в ВИ в соответствии с АВЗ.1, АВЗ.2 [Там же. С. 73–74]. При реализации соответствующих мер должны обеспечиваться:

– проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

– проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

Требования усиления. В информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты.

Т10. Требования к разбиению ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей.

В ИС должно обеспечиваться разбиение ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17 [Там же. С. 136–137].

Требования усиления. В ИС должно обеспечиваться выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией (автоматизированного рабочего места администратора управления средствами виртуализации).

Заключение. Результатом данной работы стали разработанные модель типовой ВИ, которая может быть использована при создании различных информационных систем, модель нарушителя и модель угроз и непосредственный перечень требований к системам защиты информации для таких информационных систем.

Таким образом, на основании проанализированных документов, проектов документов и приведенных в данной статье наработок можно построить информационную систему, с использованием технологий виртуализации, отвечающую требованиям основных регуляторов в сфере информационной безопасности на территории Российской Федерации.

Литература

1. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения [проект ГОСТ: разраб. ФСТЭК России]. – [Окончательная редакция]. – М., 2014. – 39 с.

2. Ледовской В.П. Виртуальным инфраструктурам – прогрессивная защита [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Progressive_Defense_for_Virtual_Infrastructures, свободный (дата обращения: 28.04.2014).

3. Securing Virtual Applications and Servers [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-network-services-uns/white_paper_c11-652663.html, свободный (дата обращения: 28.04.2014).

4. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных отрасли: методический документ Министерства связи и массовых коммуникаций Российской Федерации: одобр. решением секции №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» 21.04.2010. – 1-е изд. – М., 2010. – 50 с.

5. Меры защиты информации в государственных информационных системах: методический документ ФСТЭК России: утв. ФСТЭК России 11.03.2014. – М., 2014. – 176 с.

6. Российская Федерация. Приказы. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России №17: издан ФСТЭК России 11.03.2013. – 1-е изд. – М., 2013. – 37 с.

7. Российская Федерация. Приказы. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России № 21: издан ФСТЭК России 18.03.2013. – 1-е изд. – М., 2013. – 20 с.

Курносов Кирилл Викторович
Студент каф. информационной безопасности НГУЭУ
Тел.: 8 (913) 753-21-81
Эл. почта: kursorkvk@mail.ru

Селифанов Валентин Валерьевич
Ст. преподаватель каф. информационной безопасности
Новосибирского государственного университета экономики и управления, начальник 6-го отдела
Управления ФСТЭК России по Сибирскому федеральному округу
Тел.: 8 (383) 264-04-84
Эл. почта: sfo1@mail.ru

Kurnosov K.V., Selifanov V.V.
Development of requirements for safety assessment virtual infrastructure

In accordance with the guiding and methodological documents in the field of technical protection of information, a model was developed infrastructure, built with the use of virtualization technologies, which contains information of restricted access, not containing information constituting state secrets. Were defined the types of potential offenders security, the urgent threats, and develop a set of requirements for safety assessment of such infrastructure.
Keywords: virtualization, virtual infrastructure, virtual machine, hypervisor, information security, requirements for information security.