УДК 004.056
DOI: 10.33764/2618-981X-2019-6-2-150-158

СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, ПРИМЕНЯЕМЫЕ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Анжелика Викторовна Печенкина
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (923)706-73-23, e-mail: angelika19z78@gmail.com

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

Невозможно представить современную информационную систему без виртуализированных компонентов – серверов, удаленных рабочих мест сотрудников (VDI), сетевого оборудования. Необходим грамотный подход для защиты этих сред. Если в информационной системе компании обрабатывается информация, подлежащая обязательной защите в соответствии с требованием российского законодательства (например, персональные данные или информация, обрабатываемая в государственных информационных системах), то необходимо использовать только сертифицированные средства защиты, прошедшие процедуру оценки соответствия регуляторами – ФСБ России и ФСТЭК России. Использование этих средств защиты позволит обеспечить требуемый уровень информационной безопасности.

Ключевые слова: информационная безопасность, виртуализация, технологии, программные и аппаратные средства, хранение информации.

SECURITY SYSTEMS USED WITH VIRTUALIZATION TECHNOLOGY

Angelika V. Pechyonkina
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (923)706-73-23, e-mail: angelika19z78@gmail.com

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

It’s impossible to imagine a modern information system without virtualized components – servers, remote workstations (VDI), network equipment. The competent approach is necessary to protect these environments. If information system of a company processes information that is subjected to mandatory protection in accordance with requirements of Russian legislation (for example, personal data or information processed in state information systems), then only certified security devices that have passed the procedure of compliance assessment by regulators – the Federal Security Service of Russia and the FSTEC of Russia. The use of these protection means will ensure the required level of information security.

Key words: information security, virtualization, technology, software and hardware, information storage.

Введение

Начнем с самого понятия виртуализации. Виртуализация – набор вычислительных ресурсов и их логическое объединение, обособленное от аппаратной реализации. Такая система обеспечивает изоляцию всех логических процессов друг от друга, при этом процессы выполняются на одном физическом ресурсе.

Не стоит считать виртуализацию заведомо небезопасной – все зависит от развертывания и примененных мер безопасности. Слабая политика безопасности, а также отсутствие обучения, могут стать куда более веской причиной возникновения проблем и уязвимостей, что в свою очередь приведет к большому риску для компаний, использующих ее. Именно поэтому разработчики сертифицированных средств защиты информации выпускают специальные продукты для защиты виртуальных сред.

Технологии виртуализации несут в себе много угроз для информационной безопасности. В сравнении с физическим компьютером виртуальный аналог менее защищен. Виртуальные системы легко переносимы на другие платформы, что и является основной уязвимостью.

Системы с виртуализацией компьютеров обладают одной точкой отказа – ОС и ПО виртуализации хост-компьютера. Именно поэтому программная виртуализация редко используется в задачах обеспечения непрерывности бизнеса, так как там необходима высокая готовность и доступность информации.

Снижает защищенность также простота переносимости виртуальных систем на другие физические платформы, использование виртуальных машин в архитектуре «облачных вычислений».

Методы защиты виртуальных сред

Виртуальные системы просты в использовании и развертывании, что порождает их бесконтрольное использование в пределах инфраструктуры организации. Но часто развертываемые виртуальные системы не соответствуют требованиям корпоративной политики информационной безопасности.

Очень важно разрабатывать жизненный цикл таких систем и регулировать их миграцию, Нерегулируемая миграция виртуальной системы способна привести к нарушениям ее конфиденциальности, целостности и доступности, и в дальнейшем к росту рисков информационной безопасности (ИБ). Сама по себе виртуализация ИТ-оборудования не является механизмом ИБ.

Любое государство стремится обеспечить контроль над информацией, связанной с обеспечением национальной безопасности. Поэтому к программному обеспечению, которое поставляется на рынок и используется для построения ключевых систем информационной инфраструктуры, предъявляются особые требования.

Ранее государственное регулирование в сфере ИБ не уделяло внимания виртуализации и не предъявляло требований к защите информации, об-

рабатываемой в виртуализированной инфраструктуре. Ситуация изменилась с выходом двух приказов ФСТЭК – № 17 от 11.02.2013 и № 21 от 18.02.2013. Данные приказы предъявляют требования к защите информации, обрабатываемой в государственных информационных системах (ГИС) и информационных системах персональных данных (ИСПДн). Так же в приказах приведен список мер, которые необходимо реализовать при использовании систем виртуализации.

Но 01.06.2017 был введен в действие ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения», который напрямую относится к защите виртуальных сред, именно он позволяет в полной мере оценить соответствие требованиям государства по информационной безопасности [1].

Данный ГОСТ был разработан Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») и внесен техническим комитетом по стандартизации «Защита информации» (ТК 362).

Рассмотрим подробнее этот ГОСТ.

Вот основные термины, выделенные в ГОСТе, необходимые для понимания системы виртуализации:

Гипервизор 1 типа – устанавливается непосредственно на аппаратную платформу, к таким гипервизорам по ГОСТ относятся VMwarevSphere, Hyper-V, CitrixXenServer и пр.

Гипервизор 2 типа – устанавливается в хостовую операционную систему. К таким гипервизорам можно отнести VirtualBox, VMWareWorkstation и пр.

В ГОСТе также выделены основные объекты защиты при использовании технологий виртуализации [1]. Акцентируется внимание на том, что использование технологий виртуализации создает предпосылки для появления угроз безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации. Именно поэтому выделены основные 18 угроз безопасности, которые могут возникнуть при использовании виртуальных сред [1].

Здесь стоит заметить, что ГОСТ рассматривает именно угрозы, связанные с безопасностью виртуализации, другие угрозы безопасности не теряют актуальности, и их также необходимо рассматривать при составлении модели угроз, к примеру, угрозы, связанные с физическим доступом к инфраструктуре, организационные вопросы доступа к информации, защиты реквизитов доступа и т. д. Как мы видим из списка угроз, среда виртуализации вносит свои дополнительные угрозы, которых нет на более низком аппаратном уровне.

Таким образом, при использовании технологий виртуализации, дополнение уточненного адаптированного базового набора мер защиты можно провести исходя из требований ГОСТа.

Результаты

На данный момент, безопасность виртуальных машин (ВМ) является ключевой проблемой в их использовании и находится в центре внимания ИТ-сообщества. Платформа виртуализации состоит из множества компонентов (DHCP-сервер, NAT Device и прочие), каждый из которых становится потенциальной целью хакеров [7].

При использовании виртуальных машин в пределах инфраструктуры компании необходима точно такая же их защита, как и физических серверов. Используются точно такие же политики безопасности, как и на физических серверах. Но виртуальным сферам необходимо повышенное внимание, так как они являются самой удобной точкой для получения злоумышленником доступа к информации.

Необходимо придерживаться корпоративных стандартов по безопасности при использовании систем виртуализации, а также внимательно следить за развертыванием виртуальных машин на серверах компании и не позволять уязвимой системе работать в ее ИТ-среде. Для контроля могут использоваться такие системы, как:

– разработка компании «Код Безопасности» – vGATE;

– С-Терра Виртуальный Шлюз;

– СЗИ ВИ DallasLock.

Каждый из этих продуктов прошел процедуру оценки соответствия, что является важным критерием при выборе средств защиты информации (СЗИ). Необходимо использование именно сертифицированных СЗИ, так как достаточно обратиться к постановлению Правительства РФ № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в пункте 13 которого указано, что для обеспечения 4-го уровня защищенности персональных данных (ПДн) необходимо выполнить следующее требование:

«г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз».

К остальным уровням защищенности ПДн это требование также относится. На основании этого пункта, обязательно применение СЗИ, прошедших процедуру оценки соответствия, для нейтрализации актуальных угроз. От неактуальных угроз можно защищаться любыми СЗИ, но от неактуальных угроз никто, как правило, не защищается.

Рассмотрим подробнее особенности приведенных выше продуктов для защиты виртуальных сред.

Разработка компании «Код Безопасности» – vGATE. Данный продукт разграничивает доступ к управлению виртуальной инфраструктурой, контролирует действий привилегированных пользователей (администраторов ВИ), следит за целостностью виртуальной машины, регистрирует и проводит мониторинг со-

бытий безопасности виртуальной инфраструктуры, а также выполняет требования и рекомендации по защите виртуальной инфраструктуры. Сертифицирован по Приказам ФСТЭК № 17 (ГИС) и № 21 (ИСПДн), и по рассмотренному ГОСТ Р 56938-2016 «Защита информации при использовании технологий виртуализации».

Возможности vGATE:

– аутентификация администратора;

– создание политики безопасности, политика применяется на основе меток, применимых к серверу виртуализации, хранилищу, виртуальной машине, физическому сетевому интерфейсу, виртуальной сети, пользователю;

– проверка целостности компонентов ВМ;

– принцип двух персон при изменении конфигурации ВМ, изменение не вступит в силу, пока не будет подтверждено администратором ИБ;

– запрет создания снапшотов, запрет клонирования ВМ, гарантированное удаление информации из хранилища, контроль подключаемых устройств, контроль доступа к консоли ВМ, контроль скачивания файлов из ВМ;

– включение режима HostLockdown, запрет подключения USB-устройств к хосту, запрет SSH-подключения к хосту, настройка журналирования ВМ, контроль используемых на хосте приложений, контроль разделения управляющей и «боевой» сетей;

– поддержка отправки событий безопасности по протоколу syslog, подробная настройка событий, которые отправляются на syslog-сервер, отправка информации о произошедших событиях на почту через SMTP.

Продукт С-Терра Виртуальный Шлюз, представляет собой программный комплекс С-Терра VPN 4.2 – шлюз безопасности, функционирующий в виртуальной машине, созданной в одном из наиболее популярных гипервизоров (VMwareESXi, CitrixXenServer, MicrosoftHyper-V, KVM, HuaweiFusion). Предназначен для работы в виртуальной среде и защиты как периметра облачной инфраструктуры, так и взаимодействия между отдельными виртуальными машинами. Для безопасного удаленного доступа на конечные устройства пользователей устанавливаются программные средства защиты: С-Терра Клиент (если сотрудник использует устройство под управлением ОС Windows) или С-Терра Клиент-М (для ОС Android). Для защиты филиальной сети и/или ЦОД может также использоваться С-Терра Виртуальный Шлюз, а при отсутствии виртуальной инфраструктуры – традиционный ПАК С-Терра Шлюз. Компоненты решения реализуют криптографическую защиту информации и функции межсетевого экранирования. С-Терра Виртуальный Шлюз встраивается непосредственно в виртуальную среду и позволяет организовать защиту привычных пользовательских сервисов без ущерба удобству и функциональности. Продукт сочетает в себе широкий набор функций по защите данных при их передаче по открытым каналам связи и позволяет оперативно решать поставленные задачи. Благодаря использованию международных стандартов IKE/IPsec и применению отечественных криптоалгоритмов, передаваемый трафик шифруется по ГОСТ 28147-89, а также производится усиленная аутентификация по ГОСТ Р 34.10.

Все компоненты сертифицированы ФСБ России и ФСТЭК России для защиты конфиденциальной информации и персональных данных.

Возможности продукта:

– настройка VRRP кластера – единый интерфейс настройки основного сценария отказоустойчивости;

– расширенные диапазоны значений параметров keepalive, что дает возможность более быстрого перестроения защищенных соединений в различных схемах отказоустойчивости;

– задание адреса партнера DNS именем, что позволяет указать в конфигурации партнера без привязки к IP-адресу;

– получение CRL по HTTP, т. е. более тесная интеграция с PKI сервисами;

– задание локального адреса для построения туннелей. Независимость конфигурации шлюза от адресов внешних интерфейсов дает возможность построения более гибких сценариев с несколькими провайдерами;

– работа с файлами. Теперь работа осуществляется непосредственно в консоли конфигурирования, без перехода в консоль операционной системы;

– задание адреса источника для команды ping. Проверку и поиск неисправностей теперь можно проводить непосредственно в консоли конфигурирования, без перехода в консоль операционной системы;

– просмотр информации о защищенных соединениях. Добавлены команды просмотра информации о IKE и IPsec туннелях. Теперь просмотр осуществляется непосредственно в консоли конфигурирования, без перехода в консоль операционной системы.

Рассмотрим еще один продукт – vSphereESXi – это специализированный аппаратный гипервизор. ESXi устанавливается непосредственно на физический сервер и разделяет его на несколько логических серверов.

В 2013 г. компанией «СИС груп» был получен сертификат ФСТЭК России № 2900 на программный комплекс VMwarevSphere 5.1. Стоит отметить, что до недавнего времени это была единственная сертифицированная по требованиям безопасности версия VMware. В версии 5.5 произошли некоторые изменения, такие как двукратное увеличение конфигурационных максимумов и упрощение настройки конфигурации для приложений, чувствительных к задержкам. Также объем виртуального дискового пространства VMDK (VirtualMachineDisk) увеличился до 64 ТВ. Версия 5.5 является наиболее стабильной и востребованной.

Средства управления аппаратным гипервизором ESXi встроены в ядро VMkernel, благодаря чему объем необходимого дискового пространства сокращается до 150 Мбайт. Это значительно снижает уязвимость гипервизора к атакам вредоносного ПО и сетевым угрозам и, как следствие, делает его более надежным и безопасным. Для мониторинга оборудования и управления системой vSphereESXi использует модель интеграции партнерских API-интерфейсов без агентов. Задачи управления выполняются через интерфейс командной строки vSphereCommandLineInterface (vCLI) и интерфейс PowerCLI, который использует командлеты WindowsPowerShell и сценарии для автоматизации управления.

И, наконец, СЗИ ВИ DallasLock – это система защиты информации в виртуальных инфраструктурах, предназначенная для комплексной и многофункциональной защиты конфиденциальной информации от несанкционированного доступа в виртуальных средах на базе VMwarevSphere. Она соответствует требованиям ФСТЭК России:

– по 5 классу защищенности СВТ от НСД: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992);

– по 4 уровню контроля отсутствия НДВ: «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999).

Особенность СЗИ ВИ DallasLock, состоит в том, то он предназначен для защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, 1 класса защищенности и для защиты информации в значимых объектах критической информационной инфраструктуры до 1 категории включительно.

Ключевые возможности:

– идентификация/аутентификация администраторов и пользователей в виртуальной среде;

– разграничение доступа к объектам файловой системы и устройствам в виртуальной среде,

– регистрация событий безопасности в виртуальной среде и гибкая настройка аудита гипервизора;

– фильтрация сетевого трафика в виртуальной среде по предустановленным правилам с возможностью их редактирования или гибкой настройки;

– возможность гибкого управления квотами на количество физических процессоров.

На российском рынке информационной безопасности представлено большое количество средств защиты информации. Многим корпоративным и государственным заказчикам сложно сориентироваться в огромном количестве представленных решений и выбрать действительно качественную и эффективную защиту.

При выборе необходимо в первую очередь обращать внимание на наличие сертификатов соответствия регуляторов для формального выполнения требований по безопасности, кроме того, необходимо оценить возможность использования выбранного СЗИ в информационных системах (ИСПДн, ГИС, АСУ ТП и др.), также должна быть обеспечена совместимость продукта со средой функционирования.

Выбор в пользу разработчика с большим стажем на рынке и с достаточно «взрослым» решением снижает риски непродления сертификата, ухода продук-

та или вендора с рынка, а также может служить гарантией того, что продукт будет периодически обновляться. Следует обратить внимание на комплексные решения, когда продукт включает несколько типов СЗИ в виде модулей. Продукты разных вендоров плохо совместимы между собой, и, как правило, их одновременное применение приводит к нарушению функционирования и замедлению работы защищаемой системы. Комплексные решения, которые объединяют несколько защитных механизмов, упрощают администрирование, исключают конфликты в работе подсистем и существенно упрощают масштабируемость продукта. Рассмотренные продукты именно такими и являются, поэтому они очень популярны на рынке.

Заключение

Подводя итоги можно сказать, что виртуализация значительно упрощает работу ИТ-инфраструктуры, повышая производительность за счет оптимизации использования ресурсов, сокращения затрат на обслуживание и управление. Радикально сокращается время создания типовой инфраструктуры, и рационально используются ИТ-ресурсы, как аппаратные, так и человеческие.

Для компаний любого уровня и на любой стадии развития ИТ-инфраструктуры возможно внедрение автоматизации процессов, так или иначе связанных с выделением вычислительных ресурсов для различных подразделений внутри компании, либо для своих заказчиков. Виртуализация подходит для любой компании, стремящейся создать гибкую и современную вычислительную инфраструктуру. Простота внедрения и обслуживания, надежность и функциональность, снижение рисков для предприятия, делают обоснованными инвестиции в эту технологию. При современном уровне развития сторонних облачных систем, виртуализация открывает неограниченные возможности по объединению этих технологий и дальнейшего развития, направленного на бизнес компании, а не на постоянную заботу об ИТ-инфраструктуре.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения ; введ. 2017 – 06 – 01. – Приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-ст.

2. Елманова Н., Пахомов С. Виртуальные машины // Компьютер Пресс. – 2007. – № 9.

3. Enterprise Systems Group White paper, Page 5. Enterprise Strategy Group White Paper written and published on August 20, 2011 by Mark Peters. Архивировано 30 марта 2012 г.

4. Кирсанов В. А. Организация учебного процесса с использованием облачных технологий и технологий виртуализации. Казанский кооперативный институт (филиал) АНОО ВО ЦС РФ «Российский университет кооперации. – 2014. – № 12-3. – С. 961–963.

5. Кириллов А. Г. Особенности применения информационных технологий в управлении гуманитарным вузом // Среднее профессиональное образование. – 2013. – № 3. – С. 9–12.

6. Кириллов А. Г. Условия эффективного применения информационных технологий в управлении вузом // Преподаватель XXI век. – 2013. – Т. 1, № 2. – С. 12–15.

7. Кириллов А. Г., Гордиевских В. М., Гордиевских Д. М. Поддержка системы менеджмента качества вуза средствами информационных технологий // Зауральский научный вестник. – 2014. – № 1 (5). – С. 65–70.

8. Виртуальный Linux – Обзор методов виртуализации, архитектур и реализаций [Электронный ресурс] // IBM developerWorks Россия. – Режим доступа: http://www.ibm.com /developerworks/ru/library/llinuxvirt/index.html.

9. Виртуализация для хостинга: тупик или прорыв? [Электронный ресурс] // Администрирование серверов. Обслуживание компьютеров. – Режим доступа: http://ha-systems.ru/virtualizacija-dlja-hostinga.

10. Богданов А. В. Виртуализация: новые возможности известной технологии: Институт высокопроизводительных вычислений и интегрированных систем, 2009. – 31 с.

© А. В. Печенкина, В. В. Селифанов, 2019