УДК 004.056.52
DOI 10.21685/2587-7704-2018-3-2-11

Open Access | RESEARCH ARTICLE

Реализация мер по защите среды виртуализации, установленных нормативными документами ФСТЭК

А. Г. Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Проведен анализ возможности реализации мер защиты среды виртуализации, определенных нормативными документами ФСТЭК России. Сделан обзор установленных мер защиты среды виртуализации и анализ возможности их реализации при использовании сертифицированных средств защиты информации. Проведенный анализ показал, что существующие средства защиты информации позволяют реализовать меры защиты среды виртуализации в полном объеме. Однако количество средств защиты информации, имеющих сертификат ФСТЭК, небольшое, поэтому возможности выбора средств защиты для большинства мер защиты очень ограниченны.

Ключевые слова: информационная безопасность, меры защиты, технология виртуализации, средства защиты информации, защита среды виртуализации.

Implementation of measures on virtualized environment protection established by the regulations of FSTEC

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. An analysis of feasibility for implementing measures to protect virtualization environment, as defined by regulations of Federal Service for Technical and Export Control (FSTEC) of Russia, has been carried out. A review of the established measures to protect the virtualization environment, and an analysis of the feasibility for their implementation using certified products of information protection was made. The analysis showed that the existing means for information protection allow implementing measures to protect the virtualization environment in full. However, the amount of information protection means that are certified by FSTEC is not large; therefore, the choice of security tools for most protection measures is very limited.

Keywords: information protection, protection measures, virtualization technology, information protection means, virtualization environment protection.

Технологии виртуализации [1] были разработаны в середине 60-х гг. XX в. Однако их внедрение и практическое применение были ограничены недостаточными вычислительными возможностями аппаратной платформы, а также несовершенством программных средств. Поэтому в течение нескольких десятков лет виртуализация почти не применялась. Первые программные средства, реализующие технологию виртуализации, были разработаны в самом конце 1990-х гг. Их возможности уже позволяли применять эти средства для решения ряда практических задач, хотя этот ряд задач и был довольно ограничен. С появлением аппаратной поддержки технологий виртуализации в процессорах и с разработкой процессорных архитектур, предназначенных для построения серверов, начинается быстрое развитие технологии виртуализации и появление большого набора программных средств, предназначенных для построения среды виртуализации. При этом функциональные возможности

программных средств значительно возрастают, позволяя решать самый широкий круг задач – от создания виртуальных серверных компонент локальных сетей до построения сложных платформ, реализующих облачные вычисления или хранение и обработку больших объемов данных. По мере развития программных средств виртуализации они стали использоваться и для построения сред виртуализации, применяемых с целью обработки информации, имеющей ограниченный доступ. Для обеспечения ограничения доступа в состав функциональных возможностей были добавлены необходимые функции, а также стали разрабатываться программные и программно-аппаратные средства, предназначенные для обеспечения контроля доступа к информации, обрабатываемой в среде виртуализации и компонентам среды виртуализации.

Технология виртуализации имеет много преимуществ по сравнению с традиционным подходом к построению локальных сетей и информационных систем. Например, можно существенно сократить количество физических (аппаратных) серверов, заменив их виртуальными серверами. Сокращение происходит за счет создания виртуальных машин (ВМ), каждая из которых является виртуальным сервером, и размещения этих виртуальных серверов на одном физическом. Это, в свою очередь, уменьшает затраты на приобретение нескольких аппаратных серверов, на эксплуатацию физических серверов, например на электроэнергию. При этом количество серверов может быть увеличено за счет установки на одном физическом сервере большого количества виртуальных. Такое использование физических серверов позволяет повысить коэффициент использования ресурсов сервера, уменьшить время ввода в действие ресурсов для пользователя. Можно повысить отказоустойчивость и обеспечить бесперебойную работу виртуальной среды, установив резервный физический сервер и разместив на нем необходимые ВМ. Еще одним преимуществом технологии виртуализации является централизация управления, позволяющая создавать сложные и распределенные виртуальные среды и управлять ими.

Помимо преимуществ следует отметить ряд особенностей построения и функционирования виртуальных сред, которые создают проблемы в части обеспечения информационной безопасности (ИБ). Для пользователей создаются ВМ, имитирующие ПЭВМ с установленной в них операционной системой (ОС). Внутри ВМ помимо ОС устанавливаются приложения, используемые для обработки информации. Также внутри ВМ хранится обрабатываемая информация. Виртуальная машина представляет собой набор файлов конфигурации и виртуальный жесткий диск (как минимум один), на котором установлена ОС, приложения и хранится информация. Виртуальный жесткий диск – это файл, размер которого определен настройками ВМ. Существует возможность скопировать всю ВМ, скопировав файл жесткого диска и файлы конфигурации, и извлечь впоследствии хранящуюся информацию. Еще одним недостатком является возможность компрометации всей виртуальной среды посредством получения доступа к средствам управления или компрометации (внедрении) ВМ с установленным вредоносным программным обеспечением (ПО). Возникают и другие проблемы обеспечения ИБ виртуальных сред, для решения которых требуется применять специальные средства защиты информации (СЗИ).

В связи с широким применением виртуальных сред для обработки информации, в том числе информации ограниченного доступа, стали разрабатываться нормативные документы, устанавливающие требования к обеспечению ИБ. Так, ФСТЭК России разработала несколько положений, устанавливающих требования по обеспечению ИБ информационных и автоматизированных систем, в составе которых могут использоваться технологии виртуализации [2–4]. В этих положениях определен перечень мер защиты, которые должны применяться для защиты среды виртуализации. Сравнительный анализ перечней мер защиты показывает, что они полностью совпадают. Каких-либо отличий по составу мер защиты и их идентификации нет. Поэтому далее рассмотрен обобщенный перечень мер защиты среды виртуализации.

Нормативными документами ФСТЭК установлен следующий перечень мер защиты среды виртуализации:

– ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

– ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

– ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре;

– ЗСВ.4 Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;

– ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией;

– ЗСВ.6 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

– ЗСВ.7 Контроль целостности виртуальной инфраструктуры и ее конфигураций;

– ЗСВ.8 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;

– ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре;

– ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей.

Указанные меры защиты среды виртуализации могут быть реализованы как с использованием функциональных возможностей программных средств, применяемых для их построения, так и с использованием специальных СЗИ. Некоторые меры защиты могут быть реализованы только с использованием специальных СЗИ. Был проведен анализ возможности реализации мер защиты среды виртуализации только при использовании специальных СЗИ. Рассматривались только те СЗИ, которые имеют действующий сертификат соответствия требованиям по безопасности информации. Сведения о сертифицированных СЗИ приведены в Государственном реестре сертифицированных средств защиты информации, размещенном на официальном сайте ФСТЭК [5].

Анализ реестра показал, что сертифицированных СЗИ, которые могут применяться для реализации мер защиты информации, немного. Следует прежде всего отметить СЗИ vGate, СЗИ Гипераккорд и Аккорд-В. Эти СЗИ поддерживают две основных платформы виртуализации – Hyper-V компании «Майкрософт» и VMware vSphere компании VMware Inc. Указанные СЗИ позволяют реализовать большинство мер защиты за исключением ЗСВ.8 и ЗСВ.9, так как необходимых функций антивирусной защиты и резервного копирования не предусмотрено разработчиками. Для обеспечения антивирусной защиты могут применяться средства антивирусной защиты, разработанные для виртуальных сред, например Kaspersky Security для виртуальных сред (версия 2.0). Для реализации меры защиты ЗСВ.8 могут применяться средства резервного копирования для виртуальных инфраструктур Veeam Backup & Replication или Acronis Backup & Recovery. Кроме того, для реализации мер защиты ЗСВ.4 и ЗСВ.10 могут применяться межсетевые экраны и системы обнаружения вторжений, которые поддерживают применение в виртуальных средах.

Следует также отметить возможность использования сертифицированных СЗИ, которые специально не разрабатывались для применения в виртуальных средах, но тем не менее могут применяться для реализации мер защиты среды виртуализации. Необходимым условием является наличие поддержки той или иной платформы виртуализации, что указано в документации. Примером такого СЗИ может являться Secret Net Studio. Это СЗИ поддерживает платформы виртуализации Hyper-V и VMware vSphere.

В результате проведенного анализа возможности реализации мер защиты среды виртуализации можно сделать вывод о том, что существующие СЗИ позволяют реализовать все меры защиты, установленные нормативными документами ФСТЭК [2–4]. Количество таких СЗИ, прошедших оценку соответствия требованиям по безопасности информации и имеющих сертификат ФСТЭК, небольшое. Однако такой ограниченный набор позволяет решить задачу реализации необходимого набора мер защиты.

Библиографический список

1. NIST SP 800-125 Guide to Security for Full Virtualization Technologies. – URL: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf, свободный.
2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 № 28608).
3. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375).
4. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих по-

вышенную опасность для жизни и здоровья людей и для окружающей природной среды» (Зарегистрировано в Минюсте России 30.06.2014 № 32919).
5. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. – URL: http://fstec.ru/component/attachments/download/489 (дата обращения: 21.09.2018).

Фатеев, А. Г.

Реализация мер по защите среды виртуализации, установленных нормативными документами ФСТЭК / А. Г. Фатеев // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-11.