Васильева И.Н., Родин В.Н., Чернокнижный Г.М. Использование средств виртуализации в преподавании ИТ-дисциплин // Вестник Санкт-Петербургского университета МВД России. – № 1 (77) январь – март 2018 г. – СПб.: СПб университет МВД России, 2018. – С.148-154. http://www.univermvd.ru/files/other-files/№_1_(77)_2018_сжат.pdf

УДК 378.147.88

И.Н. Васильева, В.Н. Родин, Г.М. Чернокнижный

**Использование средств виртуализации в преподавании ИТ-дисциплин**

В статье исследуется возможность применения технологии виртуализации при организации проведения практических (лабораторных) работ по компьютерным дисциплинам. Проводится анализ существующих средств виртуализации с учетом опыта их использования в преподавании дисциплин профессионального цикла для специальности «Безопасность информационных технологий в правоохранительной сфере» в Санкт-Петербургском университете МВД России и направления подготовки «Информационная безопасность» в СПбГЭУ.

***Ключевые слова***: лабораторные работы, практические занятия, информационные технологии, виртуализация, гипервизор, виртуальная машина.

**The use of virtualization tools in teaching IT disciplines**

The article explores the possibility of using virtualization technology when organizing the practical (laboratory) works on computer disciplines. The analysis of the existing virtualization tools taking into account the experience of their use in the teaching of disciplines of the professional cycle for the specialty «Information Security in Law Enforcement» at the St. Petersburg University of the MIA of Russia and the direction of «Information Security» training in SPbSEU.

***Keywords:*** laboratory works, practical training, information technologies, virtualization, hypervisor, virtual machine.

В настоящее время в Санкт-Петербургском университете МВД осуществляется подготовка курсантов по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере». Учебный план подготовки по специальности включает ряд ИТ-дисциплин, отнесенных к профессиональному циклу, таких как «Операционные системы», «Системы и сети передачи данных», «Программирование: языки, методы и технологии», «Специальные информационные технологии в правоохранительной деятельности», «Информационные технологии в аналитической разведке», «Программно-аппаратная защита информации», «Криптографическая защита информации» и др. Преподавание этих дисциплин имеет ряд особенностей, основная их которых – необходимость закрепления теоретических знаний в ходе практической работы на компьютерах, получение навыков использования современных информационных технологий, систем и средств защиты информации. Такая работа предусматривает знакомство с широким спектром системного, прикладного и специального программного обеспечения, что существенно

влияет на уровень требований к оснащению учебных компьютерных классов и лабораторий. Хорошим решением в этой связи является использование виртуальных машин (ВМ). На сегодняшний день виртуализация стала базовой технологией не только для серьезных инфраструктурных проектов, таких, например, как центры обработки данных, облачные сервисы, но и эффективным инструментом в преподавании ИТ-дисциплин в учебных заведениях.

Использование технологии виртуализации позволяет:

- избежать необходимости физически устанавливать на компьютеры, используемые в учебных целях, все задействованные в процессе обучения программные продукты, что позволяет снизить общую нагрузку и повысить эффективность работы системы в целом;
- обеспечить приемлемый уровень требований к аппаратной части компьютеров учебных лабораторий;
- обеспечить для обучающихся и преподавателей возможность индивидуального использования заранее подготовленных ВМ как в компьютерных лабораториях, так и для самостоятельной работы в домашних условиях;
- относительно быстро включать в учебный процесс новые ИТ-системы за счет простоты создания и распространения ВМ;
- обеспечить большую степень отказоустойчивости задействованных в обучении систем, легкость резервирования информации.

Изложенные соображения применимы к преподаванию ИТ-дисциплин и для других специальностей и направлений. Рассмотрим подробнее вопросы использования ВМ в процессе проведения практических занятий с использованием компьютерных систем. Воспользуемся следующим определением. Виртуальная машина (ВМ) – виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных и которая дополнительно может содержать программное обеспечение и пользовательские данные [1].

Виртуальная (гостевая) машина предоставляет интерфейс, полностью аналогичный интерфейсу обычной (хостовой) машины. Операционная система (ОС) создает иллюзию одновременного исполнения нескольких процессов, каждого в своей (виртуальной) памяти. Существует три основных типа виртуализации [2]:

- виртуализация представлений;
- виртуализация приложений;
- виртуализация серверов и рабочих станций.

Виртуализацию представлений можно рассмотреть на примере терминальных служб Windows Server. Клиенты получают ресурсы сервера, а клиентские приложения выполняются непосредственно на сервере. Сам же клиент получает только результаты работы данного приложения.

Виртуализация приложений позволяет запускать каждое приложение в своей изолированной среде («песочнице», sandbox′е). Делается это с целью защиты системы от недоверенных или сбойных приложений. Данный тип виртуализации позволяет запускать конфликтующие между собой приложения и даже несколько версий одного приложения.

Виртуализация серверов и рабочих станций позволяет программно или аппаратно эмулировать виртуальный компьютер, имеющий, как и все компьютеры, процессор, память, жесткий диск, и т.д. Эмуляция осуществляется за счет использования монитора виртуальных машин (гипервизора).

В педагогической практике наиболее актуальным представляется использование последнего типа: виртуализация серверов и рабочих станций, так позволяет практически без ограничений создавать любую вычислительную среду для проведения занятий по ИТ-технологиям.

Рассмотрим особенности виртуализации в различных аспектах. Напомним, что гипервизоры бывают первого типа (требующие аппаратной поддержки) и второго типа (работающие как приложение поверх базовой ОС). Гипервизоры первого типа (например, VMware ESXi Server, Microsoft Hyper-V, Citrix XenServer) используются в крупных информационных системах для серверной виртуализации, позволяющей развернуть на одном физическом сервере несколько виртуальных, обеспечивая тем самым расширенный функционал системы и экономя на оборудовании, площадях, текущих издержках. В виртуализации рабочих станций они способны поддерживать сотни гостевых операционных систем. В педагогической практике гипервизоры первого типа представляют интерес, скорее как собственно предмет для изучения в некоторых дисциплинах, а не как инструмент преподавателя. Как правило, это дорогие лицензионные продукты, их сложнее устанавливать и использовать в учебных лабораториях.

Задача преподавателя состоит в том, чтобы обеспечить платформу для изучения различных ИТ-приложений, необходимых по программе данной дисциплины. До «эпохи виртуализации» все нужные приложения ставились на хостовой машине лаборатории. В результате компьютерная система оказывалась перегруженной до такой степени, что эффективность работы с ней в рамках учебного процесса резко падала. Более того, в таких дисциплинах, как «Операционные системы», «Системы и сети передачи данных», «Программно-аппаратная защита информации», где необходимо изучать различные ОС, системы защиты информации (СЗИ), системы обнаружения вторжений (СОВ), одновременная установка множества требуемых программных продуктов на одном хосте может оказаться просто невозможной. Еще одно требование при изучении указанных дисциплин – необходимость предоставление учащимся прав администратора, что делать на хостовых машинах учебных лабораторий нецелесообразно по соображениям

безопасности, обеспечения отказоустойчивости и непрерывности обеспечения учебного процесса. Здесь, как нельзя кстати, на помощь преподавателям пришли гипервизоры второго типа. Их установка на хостовой машине аналогична любому приложению, а развертывание ВМ с их помощью требует минимальной подготовки. Такую подготовку авторы проводят в форме одной из начальных практических работ «Установка и настройка ВМ» в цикле компьютерных дисциплин (например, в рамках курса «Операционные системы»). Далее в процессе занятий преподаватель должен подготовить и предоставить обучающемуся такую ВМ, которая необходима для конкретного практического занятия. На этой ВМ может быть предустановлено изучаемое приложение, либо, если это предусмотрено планом занятия, студент самостоятельно устанавливает приложение и приступает к работе с ним.

Существует ряд гипервизоров второго типа, с помощью которых можно создавать и использовать ВМ. Проанализируем их возможности с точки зрения использования в педагогической практике.

Исторически первыми и по сей день одними из самых популярных являются гипервизоры компании VMware[1]. Для использования в учебном процессе можно рекомендовать VMware Workstation pro, VMware Workstation Player, VMware vSphere. Продукты VMware используются в профессиональной практике ИТ-специалистами, поэтому у обучающихся желательно сформировать навык работы именно с этими продуктами. Гипервизоры VMware работают на хостовых машинах с ОС Windows и Linux. Вместе с тем, VMware Workstation pro является коммерческим продуктом, он довольно дорог с точки зрения приобретения достаточного количества лицензий, так как линейка гипервизоров лицензируется по количеству физических процессоров хост-машин. Поэтому он доступен не в каждом учебном заведении. VMware Workstation Player бесплатен, но лишь для частного использования, а по функциональным возможностям он значительно уступает VMware Workstation pro. Он может быть рекомендован студентам в рамках самостоятельной работы. Программное обеспечение VMware vSphere – ведущая платформа виртуализации, в том числе, для создания облачных инфраструктур. Этот продукт значительно более дорогой, чем VMware Workstation pro[2], при этом не продается без технической поддержки и подписки. Существует возможность бесплатного использования гипервизора, сопоставимого с VMware vSphere. Речь идет о бесплатном продукте VMware vSphere Hypervisor (ранее ESXi X Free). Он более сложен в управлении, чем предыдущие, и требует значительно больше ресурсов хостовой машины.

[1] Некоторое время назад компания VMware была поглощена компанией EMC, а последняя, в свою очередь, компанией Dell. Отныне VMware лишь бренд.

[2] Указать точную стоимость лицензий на продукт весьма сложно. Для тех, кому это важно, можно рекомендовать, например: http://winitpro.ru/index.php/2017/03/28/licenzirovanie-vmware-vsphere-6-5/

Кроме того, возможны ограничения на ресурсы поддерживаемых ВМ. Например, бесплатный VMware ESXi 5 позволяет использовать сколько угодно виртуальных машин на сервере с произвольным числом процессоров и ядер, однако совокупная сконфигурированная память всех включенных виртуальных машин не должна превышать 32 ГБ [3]. Справедливости ради следует отметить, что компания-производитель предоставляет ограниченные по времени версии продуктов VMware Workstation pro и VMware vSphere для свободного ознакомления. Подводя итог, можно сказать, что гипервизоры VMware доступны тем учебным заведениям, которые могут купить лицензии, имеют современный парк компьютеров и хорошую техническую поддержку в лице собственного ИТ-подразделения.

Наряду с VMware, в тройку наиболее популярных гипервизоров входят Oracle Virtualbox и Hyper-V от компании Microsoft.

Гипервизор Oracle Virtualbox по своим функциональным возможностям сопоставим с рассмотренным ранее VMware Workstation pro. Virtualbox может быть установлен на машинах с ОС Windows, Linux, Macintosh и Solaris. Продукт не имеет жестких аппаратных требований, обладает дружественным интерфейсом, прост в применении, русифицирован, постоянно обновляется, поддерживает практически все ОС и, что немаловажно – распространяется бесплатно. Поэтому он чаще всего устанавливается в учебных лабораториях, используется преподавателями для подготовки занятий, а студентами для самостоятельной работы. В дальнейшем примеры создания и использования ВМ в учебном процессе в этой статье будут проиллюстрированы именно для Virtualbox.

Основной вендор по продвижению ОС для рабочих станций, используемых в учебных заведениях, компания Microsoft, также предлагает свои решения в области виртуализации. Сразу после появления гипервизора VMware компания Microsoft разработала и выпустила на рынок сопоставимый с ним по возможностям гипервизор Virtual PC. В силу доступности и свободной интеграции с ОС Windows это приложение сразу стало использоваться преподавателями, в том числе, авторами, в учебном процессе [4]. Основным недостатком Virtual PC является поддержка только операционных систем Microsoft. Однако в настоящее время компания Microsoft отказалась от поддержки этого приложения в пользу гипервизора Hyper-V для 64-разрядных ОС – также свободно распространяемого и поставляемого в составе ряда операционных систем Windows. Вначале Hyper-V входил только в серверные ОС, начиная с Windows Server 2008R2 (как роль), что сужало возможность его использования в учебном процессе. Но, начиная с ОС Windows 8, гипервизор стал входить и в состав десктопных ОС (версий Pro и Enterprise). Обновленные версии Hyper-V поддерживают создание гостевых ОС Windows, начиная с XP SP2 и позднее, а также Linux-систем, FreeBSD, Red Hut, Ubuntu, Debian. Этот список скромнее, чем у гипервизоров,

рассмотренных выше. При этом Linux-системы поддерживаются с ограничениями. Большое количество «оговорок», указанных в мануалах по установке Linux-систем, например, в части доустановки драйверов, указывает на неудобство использования Hyper-V для данного семейства ОС. Ведь в учебном процессе требуется скорость и простота развертывания ВМ. Интерфейс гипервизора хотя и не сложен, но уступает по доступности рассмотренным выше VMware Workstation и Virtual Box. Кроме того, Hyper-V предъявляет определенные системные требования: наличие 64-битового процессора, поддержка процессором преобразования адресов второго уровня (SLAT), поддержка и включение в BIOS технологии аппаратной виртуализации и аппаратного предотвращения выполнения данных (DEP) [5]. Проверка совместимости оборудования может быть проведена с помощью системной утилиты systeminfo. Основным же преимуществом Hyper-V является высокая производительность гостевых ОС. В целом Hyper-V ориентирован на работу в корпоративных локальных вычислительных сетях (ЛВС). В итоге Hyper-V может быть рекомендован к использованию в учебном процессе в тех случаях, когда компьютерные лаборатории оснащены современным оборудованием на базе 64-разрядных процессоров, в качестве хостовых систем используются ОС Windows 8/ 8.1/ 10 и предполагается изучение программного обеспечения только на базе Windows-систем. В остальных же случаях предпочтительнее, на наш взгляд, установить Oracle Virtual Box.

Возможность использования гипервизоров не ограничивается тремя рассмотренными семействами. Неплохо зарекомендовали себя свободно распространяемые Parallels Workstation от компании Parallels, а также Qemu – бесплатный инструмент с открытым исходным кодом для эмуляции и виртуализации работы ОС на компьютере, разрабатываемый в рамках проекта Linux KVM (Kernel-based Virtual Machine).

Продукт Parallels Workstation позволял пользователю создавать неограниченное число виртуальных машин на компьютерах с Windows или Linux. Это решение поддерживало большинство дистрибутивов Windows и Linux как в качестве основной, так и в качестве гостевой ОС. Функционально и по интерфейсу программа напоминает Virtual Box. Очень похожа также инсталляция гостевой машины. Однако поддержка гипервизора была прекращена, хотя он и доступен к использованию для виртуализации устаревших ОС (последняя из которых Widows 7). Пришедший ему на смену Parallels Desktop [6] является коммерческим продуктом и ориентирован на macOS в качестве хостовой системы – с тем, чтобы запускать на ней виртуальные ОС Windows и Linux и доступные для них приложения. Благодаря «узкой специализации» он более удобен для macOS, чем, например, Virtual Box и может быть рекомендован в случае использования компьютерной техники от Apple.

Qemu может работать в среде Windows, Linux, MacOS и даже на Android, т.е. достаточно универсален. Не вдаваясь в подробности архитектуры Qemu, отметим, что сборка и установка QEMU выполняется в интерфейсе командной строки с помощью стандартных текстовых редакторов Linux (обычные этапы создания диска, задания памяти, выбора образа ISO и т.д.) [7]. Таким образом, Qemu может быть рекомендован лишь тем преподавателям и студентам, которые имеют опыт подобной работы, для остальных программа вряд ли подойдет.

Рассмотрим теперь основные моменты в использовании гипервизоров и созданных на их базе виртуальных машин в практике проведения лабораторных работ.

В среде пользователей ВМ, в том числе преподавателей, появилось не формальное деление «виртуалок» на «легкие» и «тяжелые». Эту степень определяют, в первую очередь, по размеру диска виртуальной машины. К «легким» относят старые Windows до XP включительно (диск чистой XP Professional\32 – без установленных приложений – около 1.5 ГБ) и UNIX-потомки (Debian, Ubuntu, FreeBSD, Solaris и др.), которые в «чистом виде весят» 1-2.5 ГБ. К «тяжелым» относят ОС Windows 7 и старше, серверные версии Windows, Ubuntu, RedHut. Размер дисков начинается с 5.5 ГБ и более. Сильно «потяжелеть» ВМ (даже «легкие») могут при установке на них приложений. Например, Windows Server 2016 с диском 9.5 ГБ после установки роли контроллера домена вырастает более чем на 5 ГБ. Машина Windows Server 2008R2 с SQL Server 2012 имеет диск порядка 20 ГБ. Для «переноски» файлов такого размера потребуется внешний жесткий диск или флэш-накопитель достаточного объема, размеченный в файловой системе exFAT или NTFS. Эти моменты необходимо учитывать при подготовке ВМ для конкретной учебной дисциплины. Данные по объему дисков авторами приведены для гипервизора VirtualBox. Как показывает практика, размер виртуального жесткого диска определяется типом гостевой ОС, а от типа самого диска и типа гипервизора практически не зависит.

Гипервизоры создают и поддерживают несколько типов (расширений) дисков ВМ. В частности, VirtualBox может создавать следующие типы дисков:

- VDI (VirtualBox Disk Image) – формат диска VirtualBox, используемый по умолчанию;
- VMDK (Virtual Machine Disk) – формат дисков VMware;
- VHD, VHDX (Virtual Hard Disk) – формат дисков VPC и Hyper-V;
- HDD (Parallels Hard Disk) – формат дисков Parallels;
- QED (QEMU enhanced disk) – формат для QEMU/KVM;
- QCOW (QEMU Copy-On-Write) – формат для QEMU (qcow2).

Если не планируется использовать создаваемый виртуальный диск с другими гипервизорами, можно оставить формат VDI. Отметим, что формат

VHD успешно работает на гипервизоре VPC, но Hyper-V требует для своего использования диски, созданные непосредственно в нем. Поэтому диск VHD, созданный в VirtualBox может не работать с Hyper-V без дополнительной установки сервисов интеграции.

Некоторые гипервизоры имеют возможность экспортировать и импортировать ВМ из одной среды виртуализации в другую с использованием открытого стандарта для хранения и распространения виртуальных машин OVF (Open Virtualization Format) в его формате OVA. Диск ВМ, созданный, например, в VMware и экспортированный в OVA, может быть затем импортирован в VirtualBox и запущен как ВМ в его среде. Эта возможность заявлена для всех ведущих гипервизоров: VMware, VirtualBox, Hyper-V.

У «тяжелых» ВМ есть еще одна важная характеристика, которая может ограничить их использование: объем необходимой для их работы оперативной памяти. Например, ВМ с ОС XP Professional хорошо работает при выделении ей оперативной памяти объемом 128 МБ, а работа с Windows 7 при минимуме 512 МБ будет заметно менее эффективна. Как правило, для обеспечения учебного процесса с использованием ВМ вполне достаточно компьютеров с объемом оперативного запоминающего устройства (ОЗУ) 4 ГБ. Однако если нужно смоделировать сеть из нескольких ВМ, то для «тяжелых» машин понадобится хостовый компьютер с большим объемом ОЗУ: 8 ГБ и более. Но у «легких» ВМ остается перспектива в проведении лабораторных работ. Поэтому в тех случаях, когда платформа не имеет большого значения, а важно изучить устанавливаемое на ней приложение, например, СЗИ, СОВ, можно, по мнению авторов, использовать «легкие» ВМ.

Все рассмотренные гипервизоры дают возможность запускать ВМ в нескольких сетевых режимах. При этом одним из наиболее важных моментов при планировании использования виртуальных машин для работы с внешней сетью являются соображения безопасности. Для примера будем использовать терминологию VirtualBox.

По умолчанию гостевая ОС подключается к сети с использованием технологии трансляции сетевых адресов – Network Address Translator, режим «NAT». В этом случае в хостовой ОС работает независимый DHCP-сервер, который назначает внутренние IP-адреса виртуальным машинам в пределах сети хоста 10.0.X.0 (как правило, адрес начинается с 10.0.2.15, маска 255.255.255.0). Виртуальная машина может инициировать соединение во внешнюю сеть посредством специального сервиса, осуществляющего преобразование IP-адресов. При таком типе сетевого взаимодействия ВМ используют один IP-адрес хостовой системы, они не видны из внешней сети и не могут взаимодействовать между собой, поскольку все сетевые соединения изолированы друг от друга. Пользователь и программное обеспечение работают с сервисами внешней сети, не предоставляя при этом во внешнюю сеть свои сервисы. Если при изучении определенного приложения достаточно

выхода в Интернет, никаких дополнительных настроек гостевой ОС и хоста в этом режиме не потребуется.

В режиме «Сеть NAT» ВМ могут взаимодействовать между собой, имеют выход в Интернет, но остаются закрытыми со стороны внешней сети. По сути, это – расширенный режим «NAT».

В рассмотренных режимах ВМ не смогут взаимодействовать в рамках ЛВС. Для такого взаимодействия нужно выбирать другой тип подключения – «сетевой мост». При выборе этого режима нужный сетевой адаптер должен определиться автоматически. ВМ получают IP-адрес от сервера DHCP корпоративной сети, могут выходить в ЛВС, в Интернет и взаимодействовать между собой. Этот способ является основным для проведения лабораторных работ, связанных с решением сетевых задач, но могут возникнуть ситуации, когда от режима «сетевой мост» следует отказаться. В частности, если по ходу работы необходимо установить на виртуальном контроллере домена роль сервера DHCP, то при завершении установки эта ВМ станет полноценным сервером корпоративной сети и будет раздавать IP-адреса из своего пула всем компьютерам сегмента ЛВС, а не только тем, для которых это предусмотрено практической (лабораторной) работой. Это может привести к сбою в работе сторонних компьютеров в части доступа в Интернет и к общедоступным серверам. Также не рекомендуется использовать этот режим при изучении СЗИ, СОВ, моделировании сетевых атак и т.п.

Для подобных случаев существует режим «внутренняя сеть» (рис. 1). Созданные и запущенные на гипервизоре данного хоста ВМ будут взаимодействовать в пределах хоста как изолированная сеть без выхода в ЛВС и глобальную сеть. Компоненты внешней по отношению к хосту сети так же не имеют к ним доступа. Служба автоматической частной IP адресации (Automatic Private IP Addressing, APIPA) хоста автоматически выдаст всем ВМ IP-адреса из своего пула: 169.254.X.X, маска 255.255.0.0.

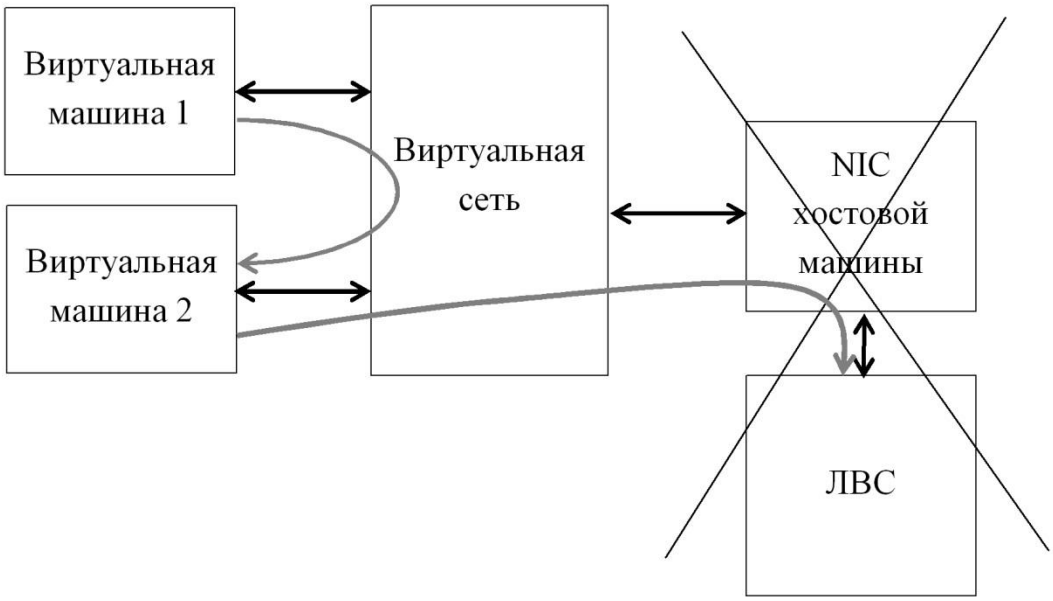


Рис. 1. Взаимодействие ВМ в режиме «внутренняя сеть»

Остальные режимы используются реже.

В режиме «виртуальный адаптер хоста» создается подсеть 192.168.56.0 между хост-системой и виртуальными машинами для обмена данными напрямую, как через коммутатор, без физического сетевого адаптера. Внешнего интерфейса с ЛВС и Интернетом нет. По использованию сходен с внутренней сетью.

Режим «универсальный драйвер» использует драйверы специальных типов, входящие в пакет расширений VirtualBox. Практического значения для преподавания этот режим не имеет.

К важным настройкам гипервизоров для использования в педагогической практике относятся создание общих папок между ВМ и хостом, а также подключение флэш-накопителей к гостевой машине. Настройки ВМ для решения этих задач просты, интуитивно понятны и не требуют комментариев (за исключением серверных версий Hyper-V, для которых предварительно должен быть включен режим расширенного сеанса [8]). Указанные функции требуются для установки приложений на ВМ, сохранения студентом результатов лабораторной работы и написания отчета по ней, так как заявленные функции общего буфера обмена между хостом и гостевой ВМ в большинстве гипервизоров, к сожалению, не работают или работают частично.

Еще одним ограничением ВМ безотносительно к используемому гипервизору, является отсутствие поддержки флэш-накопителей (USB-токенов, смарт-карт) в загрузочной среде. Это ограничение затрудняет изучение с использованием ВМ отдельных СЗИ, требующих аппаратной

(двухфакторной) аутентификации на этапе загрузки ОС. Вместе с тем, аппаратная аутентификация приложению остается доступной для изучения, хотя и может потребовать дополнительной настройки ВМ.

В заключение обратим внимание на вопросы обеспечения безопасной работы с ВМ в учебном процессе. Подход к безопасности здесь несколько иной, чем при работе в производственной ЛВС [9]. Известно, что при использовании виртуализации количество возможных уязвимостей возрастает, а традиционные внешние угрозы (такие как вирусное заражение, DoS / DDoS атаки, переполнение буферов, SQL-инъекции, XSS, и т.д.) остаются [2]. Поэтому общим требованием, позволяющим снизить вероятность внешних угроз, является минимизация работы ВМ в режиме сетевого моста, когда пользователи выходят в Интернет. Если такая необходимость существует и обусловлена учебным процессом, требуется предпринять достаточные меры безопасности, такие же, как и для обычной (хостовой) машины: использовать сильные пароли, включить брандмауэр, установить антивирусный пакет (например, из числа бесплатных: Avast, Avira, MS Endpoint Protection и др.), стараться не работать в сети Интернет под административной учетной записью и т.п. В случае, если ВМ в результате атаки окажется пораженной, это может привести к выходу из строя не только хостовой машины, на которой она развернута, но и всей сети учебного заведения. Если поражена только сама ВМ, то ее восстановлением заниматься не имеет смысла: проще и быстрее удалить ВМ и установить копию, которая всегда иметься в распоряжении преподавателя или в ИТ-подразделении. Аналогично следует поступать и в случаях реализации внутренних угроз, которые исходят от обучающихся: компрометация, перемещение, удаление, появление неуправляемых, неизвестных ВМ – все проявившиеся негативные моменты легко устраняются ИТ-специалистами или самим преподавателем путем создания аналогичной ВМ с использованием существующего виртуального диска.

Итак, можно сделать вывод, что использование ВМ значительно повышает эффективность занятий в части изучения большего количества операционных систем и приложений, скорости их развертывания, динамики проведения учебного процесса. Достоинства ВМ значительно превосходят те недостатки, о которых говорилось выше. Из рассмотренных гипервизоров, на основе практического опыта авторов, наибольшей доступностью и эффективностью обладает Oracle Virtualbox.

*Список литературы*:

1. ГОСТ Р 56938–2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения. – М.: Стандартинформ, 2016. – 31 с.

2. *Евелев, Ю.Е., Чернокнижный, Г.М.* Уязвимости мониторов виртуальных машин // Научно-технический вестник СПб ГУИТМО. – 2011. – вып.2(72). – С.149-153.
3. Бесплатный VMware ESXi 5 - новые ограничения и немного новых возможностей, 18.07.2011 [электронный ресурс]. URL: http://www.vmgu.ru/news/vmware-esxi-5-free (дата обращения 21.01.2018).
4. *Чернокнижный, Г.М.* Использование средств виртуализации пользовательских операционных сред в самостоятельной работе студентов. – Материалы учеб.-метод. конф. проф.-преп. состава 20 января 2011г. / Инновационные методы уровневого образования в университете – СПб.: СПбГИЭУ, 2011. – С. 356-358.
5. Требования к системе для Hyper-V в Windows 10, 02.05.2016 [электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/virtualization/hyper-v-on-windows/reference/hyper-v-requirements (дата обращения 21.01.2018).
6. Parallels Desktop для Mac [электронный ресурс]. URL: https://www.parallels.com/ru/products/desktop/ (дата обращения 21.01.2018).
7. *Джонс, М.* Эмуляция систем с помощью QEMU, 18.01.2008 [электронный ресурс]. URL: https://www.ibm.com/developerworks/ru/library/l-qemu/ (дата обращения 21.01.2018).
8. Использование локальных ресурсов на виртуальной машине Hyper-V с VMConnect [электронный ресурс]. URL: https://technet.microsoft.com/ru-ru/library/dn282274(v=ws.11).aspx (дата обращения 21.01.2018).
9. Безопасность современных информационных технологий: монография / под общ. ред. Е.В. Стельмашонок. – СПб.: СПбГИЭУ, 2012, С. 26-48, доступ в электронном виде по адресу http://infosec.spb.ru/wp-content/uploads/2014/05/Monografia_2012.pdf.