Безопасность виртуальной среды

Валерий АНДРЕЕВ,
зам. директора по науке и развитию ЗАО ИВК, к.ф.-м.н.

Игорь КОРЧАГИН,
ведущий специалист по ИБ ЗАО ИВК

Сегодня уже сложно возражать тем специалистам, которые отмечают катастрофический рост объемов разнородной информации, обрабатываемой миллионами информационных систем (ИС). Насущная необходимость выделения огромных технических ресурсов для хранения и обработки этой информации, а также обеспечения безопасного доступа к данным и качественного предоставления информационных услуг с помощью различного рода ресурсов и устройств (в том числе мобильных) способствует развитию новой парадигмы потребления ИТ-ресурсов – так называемых «облачных» вычислений (cloud computing). Различные модели облаков (SaaS, PaaS, IaaS и пр.) предоставляют пользователю различные данные в виде Internet- или Intranet-сервисов посредством использования технологий удаленного доступа и виртуализации. Термин «облачные» используется в связи с тем, что пользователю не видны все технические детали реализации данной модели доступа, то есть сами данные скрыты от него за «облаками».

Постепенный переход к новой парадигме вычислительного процесса в глобальных сетях обеспечивает устойчивую тенденцию к виртуализации информационных ресурсов. Уже на современном этапе развития «облачного» процесса выявилось его самое слабое звено – обеспечение безопасности конфиденциальной информации (в том числе и персональных данных) с учетом угроз, специфичных именно для виртуальной среды. Практически полное отсутствие нормативно-правовой базы и сертифицированных решений в сфере информационной безопасности (ИБ) виртуальной среды является прямым следствием неопределенности, сложившейся вокруг этих угроз и методов защиты от них.

Сегодня создание виртуальных инфраструктур продолжается зачастую в отрыве от решения вопросов ИБ. У создателей таких инфраструктур остается надежда, что средства ИБ можно будет «прикрутить» позже, как это бывает с ИС. И вот тут-то на первый план выходит тот факт, что в виртуальных средах имеются специфические угрозы, которые полностью отсутствуют в обычных сетевых средах. Связано это, прежде всего, с появлением такого нового объекта защиты, как гипервизор, – неотъемлемой части любой виртуальной среды. Заметим, что это ключевой объект среды, компрометация которого неизбежно приводит к компрометации всех обеспечиваемых им виртуальных машин. При этом изначальная защищенность гипервизора крайне низка, разумеется, с точки зрения известных ИБ-решений.

Тем не менее для создания новых механизмов защиты от специфических угроз виртуальной среды следует рассматривать комплекс уже известных и апробированных техник, которые, возможно, дадут искомый результат при условии их правильного применения и доработки.

Формирование виртуальной среды

Существуе, по крайней мере, два варианта исполнения виртуальной инфраструктуры:

- с автономным гипервизором, содержащим в себе необходимые компоненты ОС;
- с гипервизором на уровне базовой ОС.

Автономный гипервизор (аппаратная виртуализация) имеет встроенные драйверы устройств, модели драйверов и планировщик и поэтому не зависит от базовой ОС, так как он работает непосредственно с оборудованием (рис. 1).

На данный момент выделяют следующие автономные гипервизоры:

- VMware ESX;
- Citrix XenServer;
- Microsoft Hyper-V.

Гипервизор, функционирующий на уровне базовой ОС, – это компо-

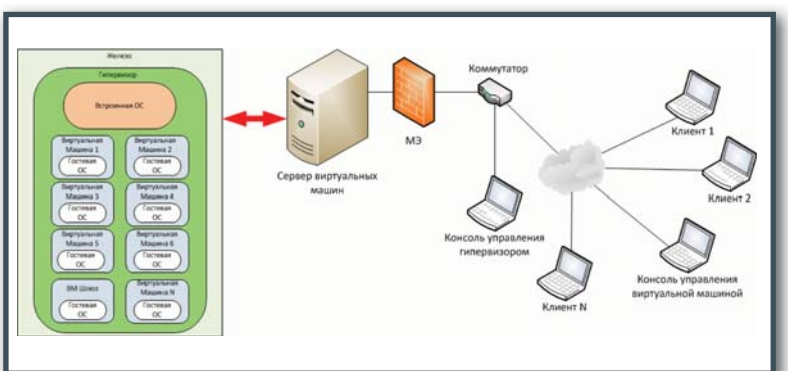

Рис. 1. Структурная схема работы автономного гипервизора

нент, работающий в одном кольце с ядром основной ОС. Гостевой код может выполняться прямо на физическом процессоре, но доступ к устройствам ввода-вывода компьютера из гостевой ОС осуществляется через второй компонент, обычный процесс основной ОС – монитор уровня пользователя (рис. 2).

На данный момент выделяют следующие существующие гипервизоры уровня базовой ОС:

- Microsoft Virtual PC;
- VMware Workstation;
- Parallels;
- VirtualBox.

Основными проблемами, которые призваны решать средства контроля несанкционированного доступа (НСД) и сохранения неизменности вычислительной среды (пусть даже и виртуальной) являются:

- идентификация и аутентификация пользователя при входе в систему (мандатный механизм доступа);
- разграничение доступа к ресурсам системы (дискреционный механизм доступа);
- контроль целостности вычислительной среды.

Заметим, что реализация защиты ресурсов уровня ОС достаточно развита, имеются и нормативные документы, и сертифицированные решения. Однако почти у всех существующих ОС есть свои уязвимости, которые выявляются при применении bootkit- и rootkit-технологий. Довольно часто эти технологии функционируют как раз на уровне гипервизора. Вот почему изучение таких специфических угроз является сегодня приоритетным и, возможно, даст ответ на вопрос о защите виртуальной среды.

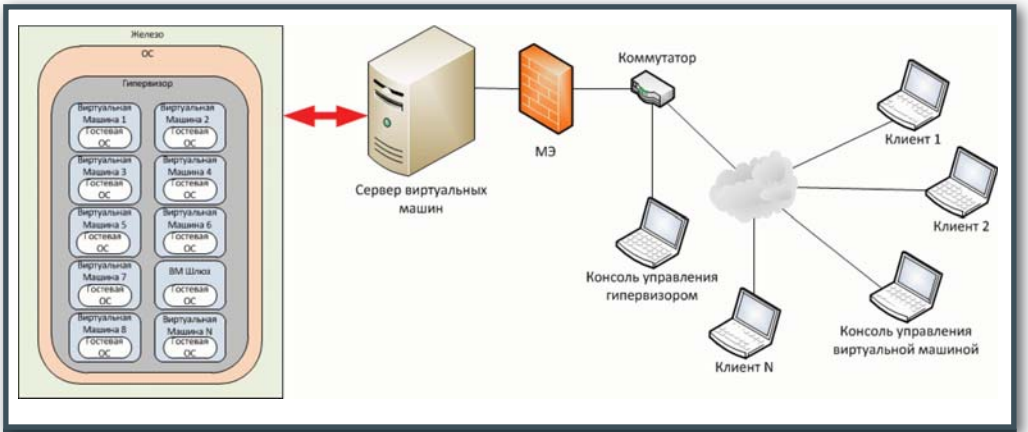

Рис. 2. Структурная схема работы гипервизора уровня базовой ОС

Виртуальное экранирование

Обе технологии виртуализации имеют близкие требования по защите информации от НСД и обеспечению безопасного межсетевого взаимодействия, но управляются по-разному. Одним из наиболее проработанных концептуально и реально механизмов защиты виртуальной среды является межсетевое экранирование, реализуемое на уровне виртуальных машин. Действительно, исходя из принципов «квази-классики», можно в первом приближении считать виртуальную среду, развернутую на конкретном аппаратном устройстве, локальной вычислительной сетью определенного ранга. Отличие очевидно: сетевой трафик между виртуальными машинами остается в пределах одного устройства и контролю со стороны известных устройств не поддается. Однако он, безусловно, существует, и применение механизма межсетевого экранирования необходимо и оправдано. Обеспечение безопасного межсетевого взаимодействия в среде виртуализации с определением периметра среды виртуальной сетевой инфраструктуры, управляемой гипервизором, показано на рис. 3.

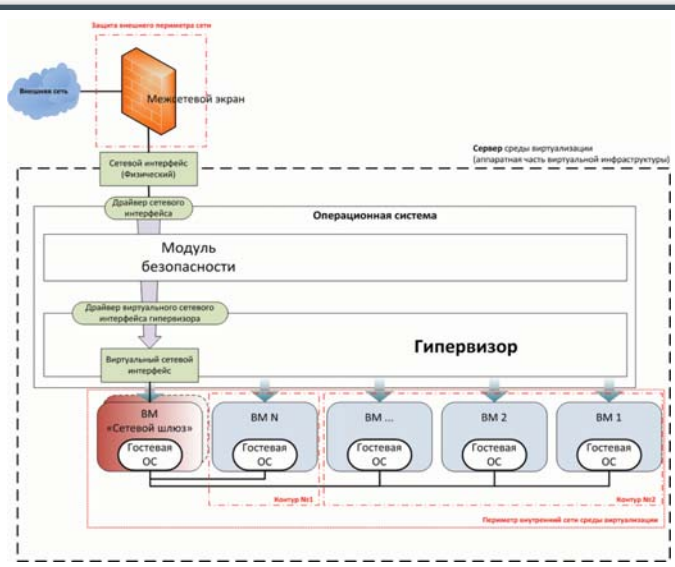

Рис. 3. Взаимодействие виртуальных машин с внешней сетью

В инфраструктуре виртуальной среды предлагается ввести дополнительную специальную виртуальную машину (сетевой шлюз) для обработки всего сетевого трафика, поступающего во внутреннюю сеть среды виртуализации (вычислительную сеть виртуальных машин). Такая виртуальная машина является виртуальным аналогом межсетевого экрана, где в качестве дополнительного функционала могут быть внедрены механизмы антивирусной защиты, DLP, IDS, IPS. Внутренняя сеть виртуальной среды может быть разделена сетевым шлюзом на контуры защиты, между которыми определяются правила безопасности межсетевого взаимодействия.

В случае выхода из строя виртуальной машины, выполняющей функции шлюза, остальные виртуальные машины останутся не затронутыми и в дальнейшем после восстановления сетевого шлюза смогут функционировать. Внедрение нескольких дублирующих сетевых шлюзов обеспечит возможность непрерывного межсетевого взаимодействия, а также балансировки нагрузки на объекты внутренней сети виртуальной среды. Таким образом, виртуальная ЛВС является двухранговой, внутреннее взаимодействие в рамках виртуального сервера понятно, остается только не забыть защитить «периметр» этой сети, то есть обеспечить функционирование межсетевого экрана самого аппаратного устройства (или их группы). Но это уже «классика».

Взаимодействие консолей управления и консолей пользователей с виртуальной инфраструктурой, а также реализация системы защиты представлены на рис. 4.

Для удаленного доступа с консоли управления виртуальными машинами

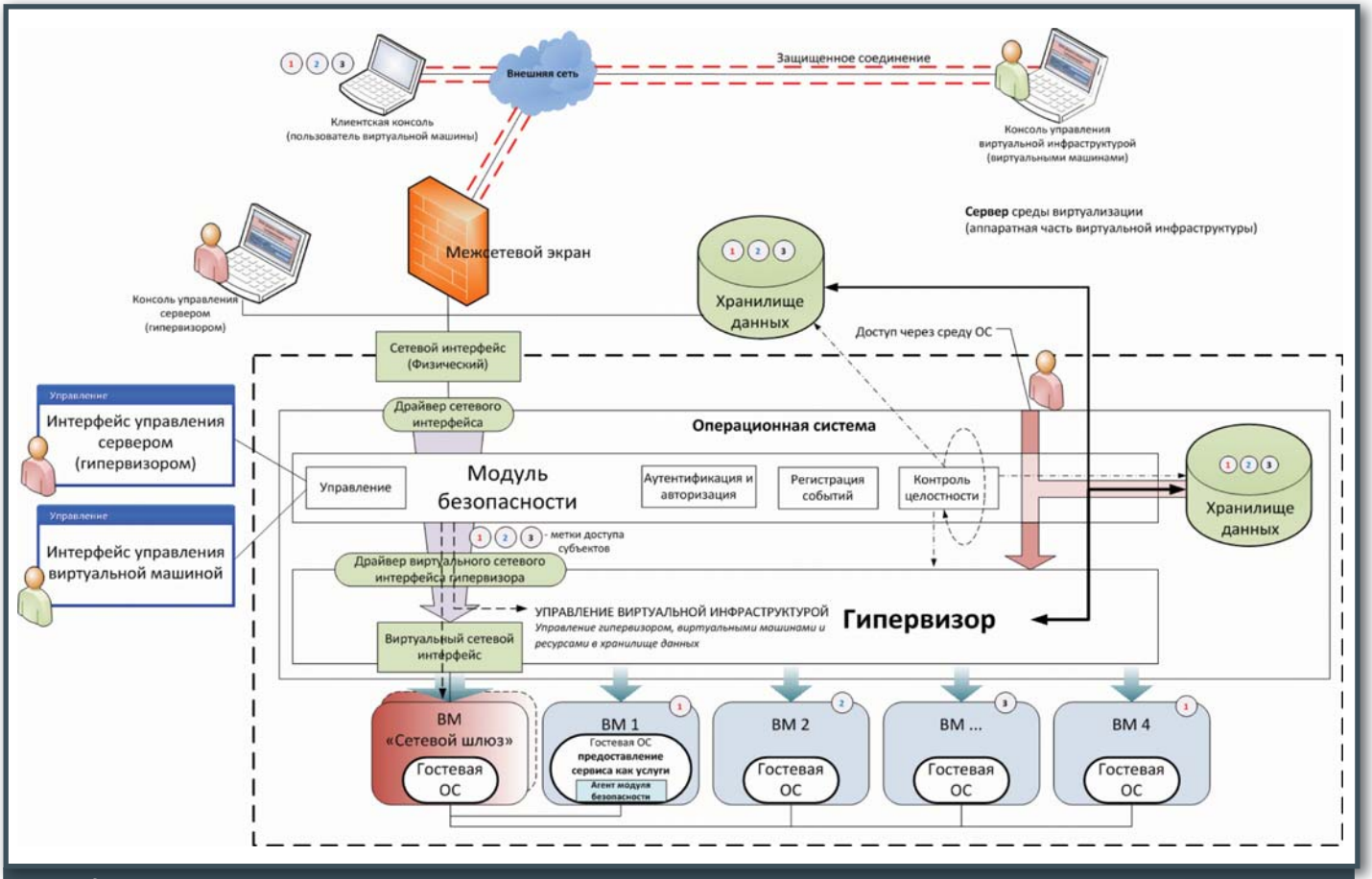

Рис. 4. Схема взаимодействия виртуальной инфраструктуры с консолями управления и пользовательским интерфейсом

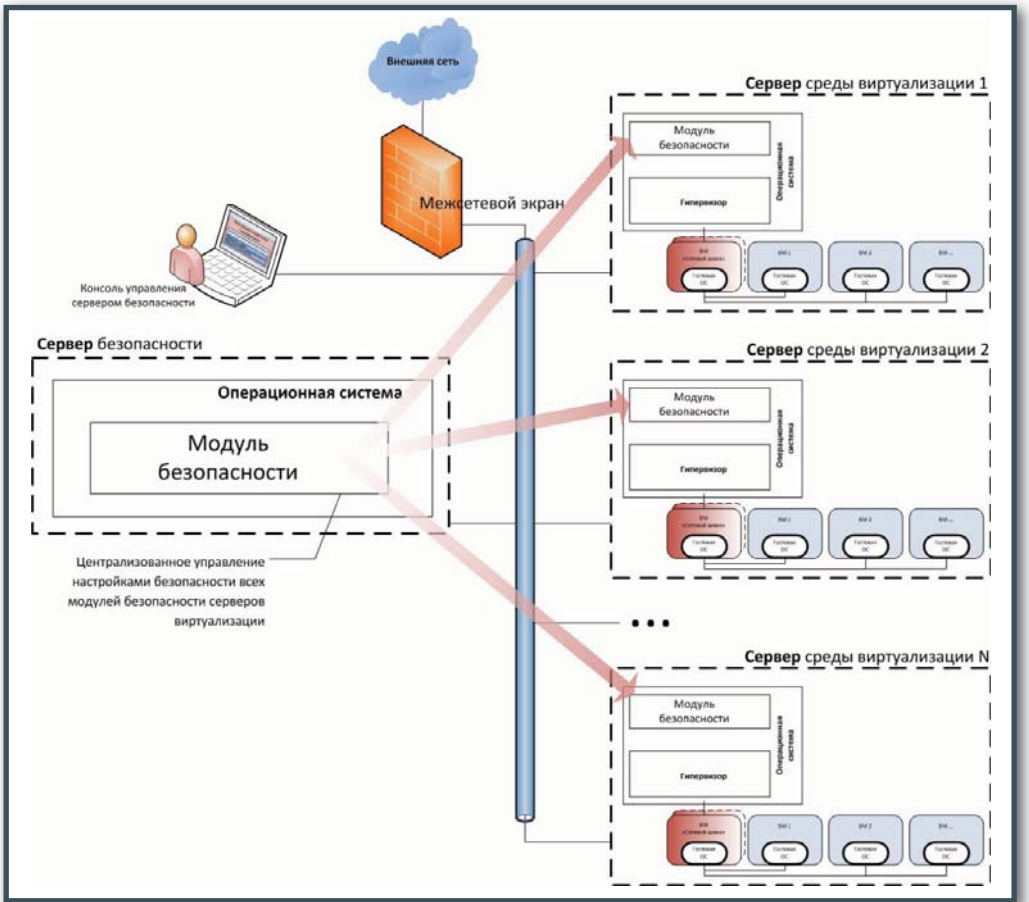

Рис. 5. Централизованное управление модулями безопасности

должно быть реализовано защищенное соединение с внутренней сетью (например, VPN- или иное соединение), в которой находится сервер с виртуальными машинами. Администрирование сервера виртуализации рекомендуется осуществлять только с консоли, напрямую подключенной к аппаратной части виртуальной инфраструктуры.

Особое внимание следует уделить созданию виртуальной защищенной среды хранения конфиденциальных данных (рис. 4), так или иначе работающей на неизменяемом разделе жесткого диска. Сетевому шлюзу также можно «вменить в обязанности» хранить настройки ВМ окружения и обеспечить контроль целостности не только самих ВМ, но и гипервизора. Если считать гипервизор «черным ящиком» с узкой функциональностью, то такой подход позволит отразить ряд угроз, являющихся специфическими именно для виртуальной среды.

Нелишним здесь будет остановиться на программных модулях доверенной загрузки (МДЗ). Это специализированные продукты, позволяющие решить указанные выше проблемы ИБ еще до старта ОС (часто оставаясь все же на уровне ОС). Использование МДЗ гарантирует вычислительному процессу неизменность, а вирту-

альной среде – авторизованного пользователя. При этом для работы с конфиденциальной информацией требуется аппаратная составляющая для хранения учетных записей пользователя (персональный МДЗ) и ВМ (серверная реализация).

Виртуальный модуль безопасности

Можно сформулировать ряд требований, которые следует выполнить для формирования нового объекта, способного обеспечивать контроль виртуальной среды. Назовем его модулем безопасности. Следует разграничить права для пользователей и выделить несколько основных должностей (ролей):

- администратор сервера (гипервизора);
- администратор виртуальной инфраструктуры (пользователь, контролирующий одну или несколько ВМ);
- пользователь среды виртуализации (виртуальной машины).

Для начала работы с виртуальной инфраструктурой необходимо пройти процедуру идентификации и аутентификации, в ходе которой будут определены права пользователя и выданы соответствующие полномочия, а также откроется возможность обрабатывать информацию в виртуальной инфраструктуре.

Доступ к информационным и системным ресурсам виртуальных машин (хранилище данных) невозможен без прохождения процедуры аутентификации, при этом запросы от гипервизора в хранилище данных (внешнее или внутреннее) осуществляются исключительно через модуль безопасности. После успешной аутентификации пользователя проходит его авторизация с целью определения полномочий доступа в соответствии с матрицей доступа.

В матрице доступа модуля безопасности определяются правила доступа субъектов (пользователей/процессов) к объектам (образам виртуальных машин, информационным данным, системным ресурсам и т.д.). Каждый объект доступа должен иметь определенную мандатную метку безопасности. Модуль безопасности должен контролировать доступ к ресурсам серверов среды виртуализации даже посредством прямого обращения к операционной системе сервера.

Для прохождения процедуры идентификации личности пользователя среды виртуализации, а также для определения его полномочий в предоставляемом конечном сервисе (прикладные задачи в среде виртуализации) в виртуальных машинах могут использоваться агенты модуля безопасности, которые передают конечному сервису полный объем сведений о запрашивающем доступ к ресурсам о пользователе. На основании данной информации сервис сам определяет полномочия пользователя в рамках задач сервиса, при этом полученные данные от модуля безопасности являются абсолютно доверенными.

Модулем безопасности также осуществляется контроль целостности гипервизора (его системных ресурсов в ОС), контроль целостности ресурсов в хранилище данных (информационных ресурсов и образов виртуальных машин), а также контроль целостности самого модуля безопасности. В модуль безопасности должны входить настраиваемые механизмы регистрации различных событий безопасности, в том числе событий управления объектами защиты со стороны администраторов.

Для виртуальных сред, где в качестве услуг предоставляются различные сервисы, доступ к которым осуществляется большим числом пользователей (например, через Интернет), возможно автоматическое формирование правил доступа пользователей в среду виртуализации на основе шаблонов безопасности.

Более высоким уровнем абстракции в виртуальной среде является сервер управления виртуальными средами, сформированными на аппаратных серверах посредством гипервизоров. Контроль этого сервера уже гораздо ближе к решению стандартных задач ИБ. Поскольку управление объектами, в состав которых входит большое количество серверов виртуализации, осуществляется с единого сервера безопасности, то настройки модулей безопасности серверов виртуализации осуществляются в центральном модуле сервера безопасности (рис. 5). Особый вопрос связан с более высокоуровневым обобществлением виртуального ресурса, когда виртуальная среда может быть представлена в виде одного компьютера с обобществленным процессором, единой памятью и пространством хранения, а также рядом внешних интерфейсов, по которым осуществляются выгрузки, печать, коммуникация и пр. Выход в «облако», таким образом, требует распределенного уже по «облаку» межсетевого экрана, антивирусных средств, средств доверенной загрузки и т.д. Этот следующий шаг виртуализации будет сделан в ближайшее время.