Александр Лысенко,
Ведущий эксперт
по вопросам защиты информации
компании «Код Безопасности»

Комплексная защита информации в виртуальной среде

Сегодня технологии виртуализации получают все большее распространение среди коммерческих и государственных структур. Однако в стремлении получить максимум от использования виртуальной ИТ-инфраструктуры, российские компании не всегда уделяют должного внимания вопросам безопасности в виртуальной среде. Этот факт находит подтверждение в отчете компании Gartner («Addressing the Most Common Security Risks in Data Center Virtualization Projects», январь 2010 г.). Там говорится, что снижение уровня защищенности виртуальной среды, зачастую, происходит по причине того, что ИБ первоначально не была включена как компонента в проект по виртуализации. При этом обеспечение должной степени безопасности данных, обрабатываемых в виртуальной среде, - важная и непростая задача.

Специфика обеспечения информационной безопасности виртуальной ИТ-среды

При внедрении технологий виртуализации стоит выделить два ключевых вопроса в контексте ИБ. Первый вопрос связан с обеспечением безопасности конфиденциальной информации с учетом угроз, специфичных для среды виртуализации; второй - с выполнением требований регуляторов в части защиты информации.

При этом виртуальная ИТ-инфраструктура обладает рядом особенностей, которые так или иначе влияют на обеспечение безопасности среды виртуализации. На что необходимо обратить внимание.

Во-первых, виртуальная машина (ВМ) представляет собой набор файлов - файлы настройки и файлы виртуальных дисков. Эти данные можно легко перенести на другое физическое оборудование путем обычного копирования. Именно поэтому наиболее опасным, хотя в большинстве случаев непреднамеренным потенциальным нарушителем, который обычно имеет неограниченный доступ к данным, является администратор виртуальной инфраструктуры. Крайне важно контролировать действия таких пользователей и по возможности ограничивать их полномочия. Для решения этой проблемы можно использовать сертифицированное решение vGate, где реализовано ролевое и мандатное управление доступом на основе меток конфиденциальности.

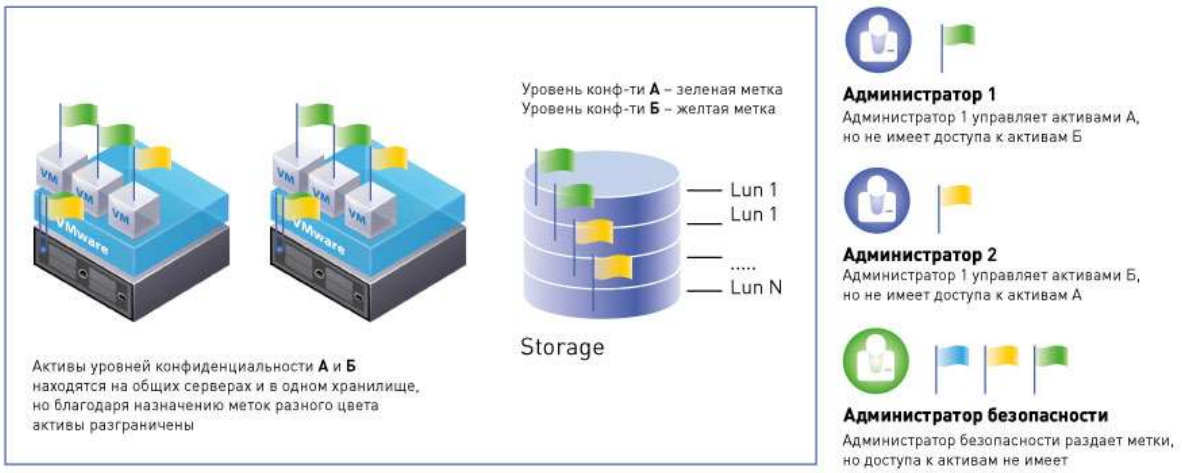

Рис.1 Разделение доступа к ресурсам с помощью меток

Во-вторых, применение технологии подразумевает появление принципиально нового объекта атаки - гипервизора. Получив доступ к гипервизору, злоумышленник автоматически получает доступ к данным на ВМ. В этом случае решение vGate обеспечит защиту от НСД самой платформы виртуализации, включая гипервизор и средства управления виртуальной инфраструктурой. При этом чтобы исключить угрозу сетевой атаки ВМ на ВМ можно использовать другие средства защиты, в т. ч. традиционные. К примеру, для защиты ВМ могут использоваться стандартные антивирусы и средства криптографической защиты. Однако в этом случае нужно помнить о возможных проблемах со снижением производительности всего комплекса виртуализации в целом. Во избежание подобных ситуаций рекомендуется применять специализированные средства защиты. К примеру, для защиты ВМ от сетевых угроз можно использовать распределенный межсетевой экран TrustAccess, который, в отличие от традиционных межсетевых экранов, фильтрует как внешние соединения, так и соединения между ВМ (трафик не покидает сервер виртуализации). Для сертифицированной защиты ВМ в соответствии с требованиями регуляторов (ФСТЭК России) можно использовать продукт Secret Net, который обеспечит разграничение доступа и доверенную информационную среду, а также защиту информации в процессе хранения. Для защиты от несанкционированного запуска программ до запуска ОС необходимо обеспечить доверенную загрузку сервера виртуализации. Для этого на каждую ВМ рекомендуется установить плату доверенной загрузки, электронный замок «Соболь» для обеспечения контроля целостности и доверенной загрузки ESX-хостов и серверов vCenter.

Особенности применения виртуализации с точки зрения действующего законодательства

В целом российское регулирующее законодательство на данный момент не делает разницы между виртуальной и физической средой обработки. Однако обработка информации в виртуальной среде имеет свои специфические особенности, которые и влияют на выполнение требований регуляторов. В любом случае, для приведения виртуальной инфраструктуры в соответствие требованиям законодательства рекомендуется учитывать специфические угрозы, характерные для среды виртуализации, определить, какие угрозы являются наиболее актуальными, и в соответствии с этим принять меры защиты (технические с применением сертифицированных средств защиты или организационные). Надо отметить, что применение сертифицированных средств защиты информации особенно важно для компаний, которые используют бухгалтерские и финансовые программы, системы управления предприятием и персоналом, CRM-системы и другие программы, обрабатывающие персональные данные.