Выводы о средствах защиты виртуализации

текст Светлана Конявская, Екатерина Шамардина

Этот текст представляет собой выводы из объемного аналитического исследования о наиболее известных на отечественном рынке средствах защиты информации (СЗИ) для различных виртуальных инфраструктур (ВИ). Критерии для сравнения СЗИ выделены с учетом требований нормативных документов[1], пожеланий владельцев ВИ и нюансов реализации в различных СЗИ базовых механизмов защиты. Выводы, не подкрепленные данными, на основе которых они сделаны, голословны. В случае вашего интереса мы предоставим материал полностью, обращайтесь к нам по адресу okbsapr@okbsapr.ru.

СЗИ ДЛЯ VSPHERE

Значительное количество требований покрывается СЗИ от разработчика, традиционно считающегося основным конкурентом ОКБ САПР. Однако для функционирования этого СЗИ необходимо разворачивание дополнительного сервера – сервера авторизации. Помимо этого, самостоятельно оно не обеспечивает разграничение доступа к ресурсам внутри виртуальной машины (ВМ) и не содержит в комплекте поставки средств доверенной загрузки (СДЗ), а значит, требуется приобретение дополнительных СЗИ. Кроме того, СЗИ функционирует только по централизованной схеме. Это незначительное, на первый взгляд, ограничение в случае отказа автоматизированного рабочего места (АРМ) управления означает полную неработоспособность СЗИ. Критичность этой особенности снижается горячим резервированием АРМ.

Еще одно популярное СЗИ зарубежного разработчика тоже работает только по централизованной схеме и, являясь средством контроля доступа к интерфейсам управления виртуальной инфраструктурой, не обеспечивает других важных с точки зрения безопасности функций, поэтому его использование для защиты виртуальных инфраструктур должно дополняться СЗИ разграничения доступа и СДЗ.

Последнее исследованное СЗИ (отечественное), также как и два предыдущих рассмотренных средства, не может самостоятельно обеспечить ряд необходимых функций и требует наличия сервера безопасности ВИ, разворачиваемого специально для СЗИ.

Наибольшее количество требований выполняется программно-аппаратным комплексом (ПАК) «Аккорд-В.». Основными его преимуществами являются:

1. Полная интеграция в существующую информационную систему.
2. Для построения полноценной системы защиты не требуется докупать и устанавливать дополнительные СЗИ разграничения доступа и СДЗ.
3. Контроль целостности ресурсов всех компонентов виртуальных инфраструктур, в том числе файлов ВМ.
4. Удобная настройка правил доступа к устройствам.
5. Обеспечение доверенной загрузки всех компонентов виртуальных инфраструктур, в том числе ВМ.
6. Возможность управления безопасностью децентрализованно, на конкретном защищаемом объекте (vCenter, ESXi, ВМ).

СЗИ ДЛЯ HYPER-V

Наибольшее количество требований выполняет ПАК «ГиперАккорд». Среди СЗИ ВИ для платформы Hyper-V ГиперАккорд выделяется, в первую очередь, полнотой предоставляемой системы защиты и программно-аппаратной реализацией, которая в совокупности с энергонезависимой памятью аппаратных компонентов позволяет сделать систему защиты максимально эффективной. Преимуществами этого комплекса также являются:

1. Полная интеграция в существующую информационную систему.
2. Возможность настройки правил доступа к устройствам.
3. Контроль целостности ресурсов всех компонентов виртуальных инфраструктур, в том числе файлов ВМ.
4. Возможность управления безопасностью децентрализованно, на конкретном защищаемом объекте.
5. Обеспечение доверенной загрузки компонентов виртуальных инфраструктур.

Остальные комплексы, участвовавшие в сравнении, универсальные – для vSphere и для Hyper-V одновременно, и они уже рассмотрены выше. Надо отметить, что такая многофункциональность, кажущаяся на первый взгляд плюсом, таит в себе существенный подводный камень, связанный со структурой процесса сертификации. Каждая дополнительно поддерживаемая операционная система (ОС) представляет собой новый объект проверок. Это обстоятельство может приводить к различным коллизиям при продлении сертификатов или инспекционных контролях. Более простые по структуре СЗИ менее проблемны с этой точки зрения.

СЗИ ДЛЯ KVM

В рамках исследования проанализированы два отечественных комплекса, обладающие в целом одинаковыми функциональными возможностями и предназначенные для того, чтобы дополнить возможности ОС. Они рассмотрены в совокупности с ОС специального назначения, необходимой для функционирования комплексов и обеспечения полноценной защиты. При их использовании необходимо применение дополнительных СЗИ, поскольку не контролируются ресурсы внутри ВМ и не обеспечивается доверенная загрузка сервера виртуализации и ВМ.

Наибольшее количество требований выполняет ПАК «Аккорд-KVM». В сочетании с рекомендуемыми для совместного применения с ним СЗИ, такими как ПАК «Аккорд-X» для сервера виртуализации и СПО СЗИ семейства «Аккорд» для ВМ, входящими в штатный комплект поставки комплекса, он позволяет построить наиболее полную систему защиты, контролирующую все компоненты ВИ. Аккорд-АМДЗ из состава ПАК «Аккорд-X» обеспечивает доверенную загрузку сервера и идентификацию/аутентификацию пользователей, а программное обеспечение (ПО) разграничения доступа, устанавливаемое в ОС сервера и ВМ, контролирует доступ пользователей к ресурсам, в том числе к подключаемым устройствам. Кроме того, для Аккорд-АМДЗ можно назначить в качестве контролируемых файлы других СЗИ. Важно, что Аккорд-KVM – наложенное СЗИ, для выполнения своих функций он не требует использования в ВМ той или иной конкретной ОС, это может быть даже Windows.

[1] *Приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Рекомендации в области стандартизации Банка России по обеспечению информационной безопасности организаций банковской системы РФ РС БР ИББС-2.8-2015.*