

# Безопасность виртуальной инфраструктуры: НОВЫЕ ВЫЗОВЫ, НОВЫЕ РЕШЕНИЯ

Константин Пичугов, менеджер по продукту компании "Код Безопасности"



**РЕШЕНИЯ** на базе виртуализации получают сегодня все большее распространение, что в общем-то неудивительно. Зрелость технологических решений этой области уже доросла до уровня промышленного использования. Кроме того, виртуальная инфраструктура позволяет вполне реально экономить на капитальных и операционных затратах. Однако в виртуальной среде возникают специфические особенности обеспечения информационной безопасности, без учета которых нельзя гарантировать сохранность конфиденциальной информации, в том числе персональных данных.

## Особенности безопасности в виртуальной среде

Обеспечение информационной безопасности ИТ-инфраструктуры предусматривает решение как минимум двух задач: обеспечение состояния конфиденциальности, целостности и доступности информации и обеспечение соответствия требованиям законодательства в отношении защиты определенных категорий информации (конфиденциальная информация, персональные данные и т.п.). Вместе с тем при обработке информации в виртуальной среде имеются свои специфические особенности, отсутствующие в физической среде:

- информация обрабатывается в гостевых машинах, кото-

рые находятся под полным контролем гипервизора, способного абсолютно незаметно для традиционных средств защиты информации перехватывать все данные, идущие через устройства;

- администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору, становится очень важным субъектом безопасности информационной системы – фактически он может получить доступ к информационным ресурсам в обход существующей политики информационной безопасности компании;

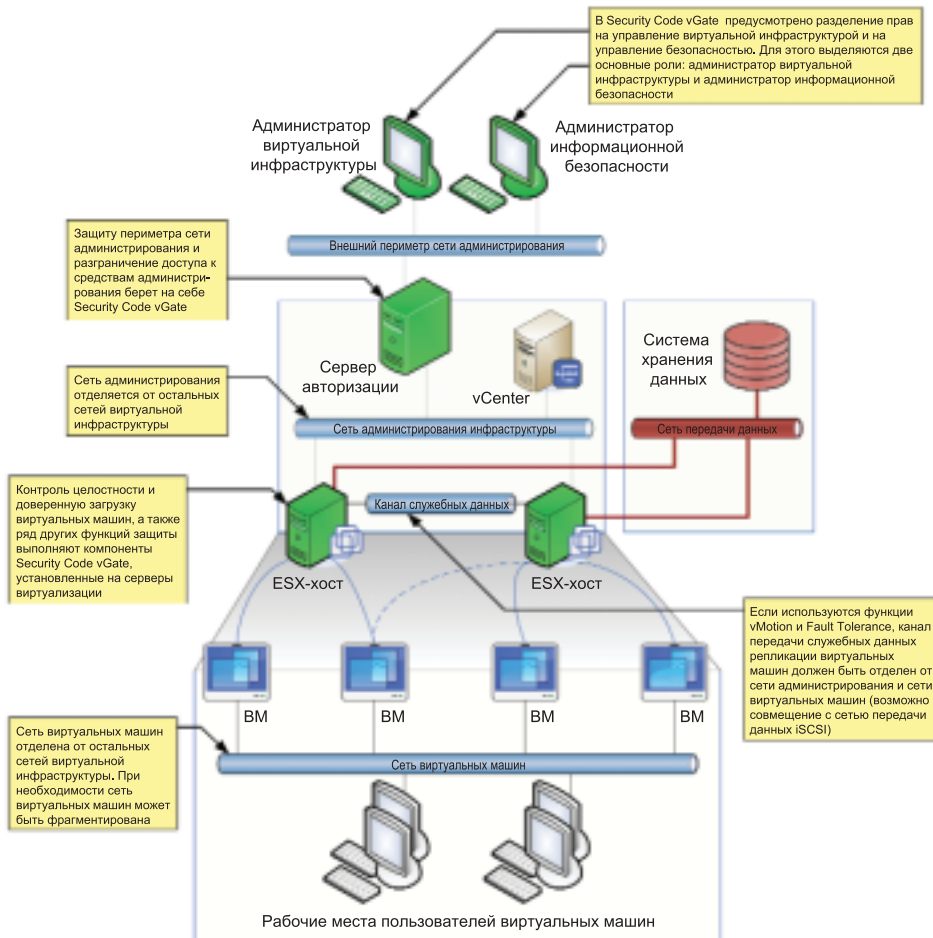
- средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки, проникновение в который дает возможность нарушителю получить доступ к гипервизорам серверов виртуализации, а затем к конфиденциальным данным, обрабатываемым на гостевых машинах;

- традиционные СЗИ, разработанные для защиты физической инфраструктуры, могут не учитывать существование гипервизора, являющегося фактически нарушителем, реализующим атаку "человек посередине" при взаимодействии гостевой машины со всеми устройствами;

- диски гостевых машин обычно размещаются в сетевых хранилищах, которые должны физически защищаться как самостоятельные устройства;

- традиционные межсетевые экраны не контролируют трафик внутри сервера виртуализации, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети. Однако этот сетевой трафик не покидает серверы виртуализации и не проходит через физические межсетевые экраны и другое физическое сетевое оборудование;

- каналы передачи служебных данных серверов виртуализации обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной памяти гостевых машин, которые могут содержать конфиденциальные данные.



Пример виртуальной инфраструктуры на основе продуктов VMware с развернутой системой защиты Security Code vGate for VMware Infrastructure (элементы инфраструктуры, содержащие компоненты продукта, выделены на схеме зеленым цветом)

Если в виртуальной среде обрабатываются данные ограниченного доступа (конфиденциальная информация, персональные данные, банковская информация, государственная тайна и т.д.), защищенность виртуальной информационной системы должна соответствовать требованиям законодательства: Федеральному закону от 27.07.2006 г. № 152-ФЗ, Постановления Правительства РФ от 17.11.2007 г. № 781. Методические рекомендации и материалы регуляторов по обеспечению безопасности персональных данных не делают различий между физической и виртуальной средой обработки данных. То же самое касается и руководящих документов регуляторов в части защиты конфиденциальной информации. В виртуальной инфраструктуре также необходимо применять сертифицированные средства защиты информации требуемого уровня защищенности и отсутствия в них недекларируемых возможностей. В этой связи особую важность приобретает профессиональное проектирование системы, причем в зависимости от категории обрабатываемых данных требуется проводить аттестацию виртуальной информационной системы.

**Средства защиты виртуальной инфраструктуры**

Виртуальная инфраструктура повышает степень интеграции вычислительных средств в информационной системе, уменьшая количество физического оборудования, но совершенно не уменьшает, а скорее увеличивает количество объектов и субъектов информационного обмена и усложняет структуру их взаимодействия. Поэтому повышать защищенность виртуальной инфраструктуры нужно комплексно путем комбинации сетевых и локальных средств защиты в ряду с интеграцией широкого набора защитных механизмов, применяемых одновременно.

Но насколько применимы традиционные СЗИ в виртуальной среде? Традиционные аппаратные СЗИ во многих случаях невозможно использовать для защиты виртуальных машин по техническим причинам. Действительно, чтобы, например, аппаратный замок мог

обеспечивать контроль целостности и доверенную загрузку операционной системы виртуальной машины, то, во-первых, поддержка данного устройства должна быть обеспечена средой виртуализации, а во-вторых, само устройство должно быть разработано с учетом использования в виртуальной среде. Что касается программных СЗИ, установленных на виртуализации, а во-вторых, операционная среда оказывается полностью скомпрометированной, если нарушитель получает доступ к средствам управления средой виртуализации. Поэтому традиционные программные СЗИ, разработанные без учета особенностей эксплуатации в виртуальной среде, зачастую не обеспечивают должный уровень защиты.

**Security Code vGate for VMware Infrastructure**

Одним из продуктов компании "Код Безопасности", нацеленным на защиту виртуализации, является новый продукт Security Code vGate for VMware Infrastructure. Это специализированное средство защиты информации, предназначенное для обеспечения безопасности управления виртуальной инфраструктурой VMware Infrastructure 3 и VMware vSphere 4. Продукт поступит на рынок в 3-м квартале этого года, а в настоящий момент можно получить доступ к тестовой версии. Для этого нужно зарегистрироваться на странице технологического партнерства компании "Код Безопасности" (<http://www.securitycode.ru/solutions/virtual/partnership/>).

Продукт Security Code vGate for VMware Infrastructure неслучайно ориентирован на защиту именно управления виртуальных инфраструктур, а не на защиту отдельных виртуальных машин. К средствам управления виртуальной инфраструктурой относятся серверы виртуализации, серверы централизованного управления виртуальной инфраструктурой, средства резервного копирования виртуальных машин и т.п. Компрометация любого из этих средств приводит к компрометации группы виртуальных машин или всей виртуальной инфраструктуры. Ценность всех вышеперечисленных элементов с точки зрения информационной безопасности очень велика. Защита их от несанкционированного до-

Компания "Код Безопасности", входящая в группу компаний "Информзащита", – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Как самостоятельная бизнес-единица компания образована в октябре 2008 г. в соответствии со стратегией группы, направленной на дальнейшее развитие собственной линейки технических средств защиты информации. Кроме задачи развития, поддержки и продвижения таких популярных продуктов, как Secret Net, "КУБ", "Континент", "Соболь", ключевой задачей компании "Код Безопасности" на ближайшую перспективу является вывод на рынок новых программных продуктов, предназначенных для управления доступом, защиты виртуальных инфраструктур и персональных данных, коммерческой и государственной тайны. Сейчас в компании "Код Безопасности" работают более 100 человек. Многие ее сотрудники начинали свою работу в группе компаний в штате Научно-инженерного предприятия "Информзащита". На данный момент команды разработчиков "Кода Безопасности" находятся в двух городах – Москве и Санкт-Петербурге.

ступа позволяет, во-первых, деактуализировать основные вышеупомянутые проблемы безопасности в виртуальной среде, а во-вторых, создать платформу для использования как традиционных, так и новых средств защиты, устанавливая их на виртуальные машины.

**Функциональность**

Какие же функции защиты обеспечивает Security Code vGate for VMware Infrastructure? Это аутентификация администраторов виртуальной инфраструктуры и разграничение доступа к средствам управления виртуальной инфраструктурой. Причем продукт берет на себя функции защиты всего периметра сети администрирования. Контроль целостности конфигурации виртуальных машин и доверенная загрузка ОС позволяет восполнить невозможность использования аналогичных функций аппаратных замков для защиты виртуальных машин. Присутствует также дискреционный механизм разграничения прав серверов виртуализации на виртуальные машины. Есть контроль целостности и доверенная загрузка серверов виртуализации, а также характерные для всех средств защиты функции аудита и контроля целостности самого СЗИ. ●



**NIM** ●  
**АДРЕСА И ТЕЛЕФОНЫ КОМПАНИИ "КОД БЕЗОПАСНОСТИ" см. стр. 80**