



Код безопасности
ГК «Информзащита»

Технологии виртуализации в коммерческих центрах обработки данных

Как обеспечить оптимальную защиту данных?

Введение

Ведущие эксперты в области проектирования ЦОД и технологии виртуализации сходятся во мнении, что применение средств виртуализации значительно повышает экономическую эффективность ЦОД за счет консолидации ресурсов. Именно поэтому в последнее время появляется все больше ЦОД, построенных с использованием технологий виртуализации.

Обеспечение должной степени безопасности данных клиентов, обрабатываемых в виртуализированных ЦОД, – важная и непростая задача. Ведь помимо обычных угроз безопасности данных в ЦОД добавляются еще и специфические угрозы, присущие виртуальной среде.

В большинстве случаев ЦОД находится вне IT-инфраструктуры предприятия. Поэтому клиентам гораздо труднее поддерживать целостность, доступность и конфиденциальность данных, а также следить за соответствием нормативным требованиям, чем при нахождении вычислительных ресурсов на территории собственной организации. Кроме того, многие проблемы в области безопасности и нормативного соответствия связаны с недостаточной прозрачностью процессов обеспечения безопасности в ЦОД.

Стоит отметить и то, что в некоторых случаях задача обеспечения безопасности ресурсов клиентов может быть возложена на владельца ЦОД. В таких случаях от клиентов требуется полностью доверить данные (в том числе и ограниченного доступа) сторонним лицам, что вызывает естественные опасения клиентов за безопасность данных, хранящихся в виртуализированном ЦОД.

Доверие клиентов – важная составляющая имиджа любого ЦОД. Для клиентов же основной потребностью является надежное и безопасное хранение их данных, а также поддержание конфиденциальности и целостности этих данных. Вот почему повышенная безопасность нередко предлагается владельцами ЦОД как дополнительная услуга.

Поскольку для ряда клиентов также немаловажной является задача обеспечения соответствия требованиям отраслевых стандартов (например PCI DSS) или требованиям ФЗ-152 «О персональных данных», то возможность предоставления такой услуги может стать неплохим преимуществом для владельца ЦОД.

В данном документе будут проанализированы специфические особенности обеспечения безопасности данных в виртуализированных ЦОД. Кроме того, будут рассмотрены возможности продукта vGate компании «Код Безопасности», с помощью которого владелец ЦОД может гарантировать клиентам оптимальную защиту их ресурсов в условиях виртуальной среды, в том числе в соответствии с отраслевыми стандартами и лучшими мировыми практиками, а также выполнение требований законодательства по защите персональных данных.

Специфика обеспечения безопасности в виртуализированных ЦОД

Основная проблема обеспечения безопасности виртуальной среды связана с тем, что традиционные средства защиты информации не способны обеспечить защиту от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры. Кроме того, привычные решения не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. Если нарушитель получает доступ к средствам управления виртуальной инфраструктурой, операционная среда традиционных средств защиты информации оказывается полностью скомпрометированной. Например, через гипервизор (компонент виртуальной архитектуры) нарушитель может незаметно для традиционных средств защиты информации, работающих в виртуальных машинах, совершать следующие злоумышленные действия:

- копировать и блокировать поток данных, идущий на все устройства (HDD, принтер, USB, сеть, дискеты);
- читать и изменять данные на дисках виртуальных машин, даже когда они выключены или не работают, без участия программного обеспечения этих виртуальных машин.

Поэтому и выполнить требования по нормативному соответствию (например, требования отраслевого стандарта PCI DSS или ФЗ №152 «О персональных данных») в условиях виртуальной среды с помощью традиционных средств защиты информации довольно затруднительно.

Другим источником проблем может стать появление в виртуализированных ЦОД нового слоя привилегированных пользователей – администраторов виртуальной инфраструктуры, обладающих самыми широкими полномочиями по манипуляции с данными клиентов (дублирование VM, получение доступа к хранилищу VM, копирование файлов VM и т. д.), в том числе и получение доступа к данным виртуальных машин клиентов. Именно поэтому крайне важно контролировать действия таких пользователей ЦОД и по возможности ограничивать их полномочия. Для устранения возможности ошибочных или злоумышленных действий со стороны администраторов оптимальным решением будет предоставление доступа к ресурсам клиента только тем администраторам, которые непосредственно занимаются настройкой и управлением ресурсами клиента, и только в минимальном для выполнения своих обязанностей объеме полномочий.

Важной особенностью виртуализации является возможность совместного хранения ресурсов разных клиентов: VM разных клиентов могут выполняться на одном сервере виртуализации, а их диски – находиться в одном хранилище. Совместное хранение ресурсов разных клиентов – источник ряда проблем, таких как потенциальный ущерб для соседей в случае компрометации ресурсов (VM) хотя бы одного клиента, а также возможность НСД к ресурсам соседа со стороны пользователей клиента. Очевидно, что эти проблемы решит разграничение (разделение) ресурсов разных клиентов, но в силу специфики виртуализации это не всегда просто.

При определенных обстоятельствах на территорию ЦОД могут получить физический доступ различные группы лиц. Это и персонал ЦОД, не имеющий непосредственного доступа к среде, и представители других организаций, арендующие стойки или серверы, представители третьих организаций и т. д. Как правило, в большинстве ЦОД эта проблема решается с помощью комплекса организационных мер. При переносе данных клиентов в виртуальную среду появляются новые каналы утечки информации, специфичные для виртуальной среды. Поэтому стандартных организационных мер для решения этой проблемы может быть уже недостаточно.

ОСНОВНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ВИРТУАЛИЗИРОВАННЫХ ЦОД:

- неэффективность традиционных средств защиты информации;
- выполнение требований отраслевых стандартов и законодательства в условиях виртуальной среды;
- возможность получения доступа администраторов поставщика услуг к данным виртуальных машин;
- совместное хранение ресурсов разных клиентов;
- повышение риска несанкционированного доступа неавторизованных пользователей к ресурсам.

Обеспечение безопасности с помощью vGate R2

vGate — оптимальное решение для обеспечения полноценной защиты ресурсов клиентов виртуализированного ЦОД, соответствия нормативным требованиям и отчетности о состоянии параметров безопасности виртуальной инфраструктуры.

vGate — оптимальное решение по обеспечению безопасности ресурсов клиентов виртуализированного ЦОД

Для решения проблемы «суперпользователя» в vGate реализовано разделение ролей пользователей. Управление виртуальной инфраструктурой закреплено за администраторами, а управление безопасностью — за администратором безопасности. В случае использования vGate администратор получает доступ к виртуальной инфраструктуре только после обязательной процедуры аутентификации в vGate. После этого все действия администратора по управлению виртуальной инфраструктурой, а значит и доступ к ресурсам клиентов виртуального ЦОД, контролируются и фиксируются в журнале событий vGate. Кроме того, полномочия каждого администратора виртуальной инфраструктуры ограничены в соответствии с его задачами администратором безопасности (например, предоставлен доступ только к необходимым серверам, запрещена/разрешена возможность скачивания файлов виртуальных машин или создания назначен-

ных заданий и т. д.). Казалось бы, тут появляется другой «суперпользователь» в лице администратора безопасности. Но этого не происходит, поскольку для этого пользователя ограничен доступ к виртуальной инфраструктуре и возможность самосанционировать доступ к виртуальной инфраструктуре отсутствует.

Для управления доступом пользователей и разделения ресурсов разных клиентов в vGate реализовано мандатное управление доступом на основе меток конфиденциальности. Пометив ресурсы разных клиентов метками разных цветов, можно гарантировать логическое отделение ресурсов одних клиентов от ресурсов других. И хотя физически эти ресурсы могут находиться на одном сервере или в одном хранилище, такое логическое отделение гарантирует то, что ресурсы одной организации или ее сотрудники не получают доступа к ресурсам другой. С помощью меток конфиденциальности можно также разграничить доступ администраторов к ресурсам клиентов: администратор без нужной метки не сможет получить доступ к этим ресурсам.

Разделение ролей на управление виртуальной инфраструктурой и управление безопасностью и контроль действий администраторов решает проблему «суперпользователя»

Мандатное управление доступом на основе меток конфиденциальности, реализованное в vGate, определяет не только доступ администратора к объектам, но и условия выполнения основных операций с ними, например, таких как:

- создание, редактирование параметров и удаление VM;
- приостановка и возобновление работы VM;
- перезапуск и завершение гостевой ОС;
- перемещение VM на другой сервер и смена хранилища VM;
- доступ к хранилищу VM;
- редактирование различных сетевых параметров VM и т.д.

Мандатное управление доступом на базе меток конфиденциальности обеспечивает:

- логическое разделение ресурсов разных клиентов;
- разграничение доступа администраторов к ресурсам разных клиентов;
- контроль конфигурации VM и серверов виртуализации

Примечательно, что для серверов виртуализации и VM метки конфиденциальности выполняют двойную роль: не только являются базой для мандатного управления доступом, но и дают возможность сопоставить этим объектам политики безопасности. Политики безопасности настраивают для конкретной метки индивидуально, после чего при назначении метки объекту (серверу виртуализации или VM) этот набор политик начинает действовать для него. Политики безопасности позволяют обеспечить соответствие требованиям PCI DSS, СТО БР ИББС, VMware Security Hardening Best Practice, CIS VMware ESX Server 3.5 Benchmark. Причем в vGate настроить такие соответствия крайне просто: достаточно включить нужный шаблон настроек при создании политики безопасности.

vGate позволяет привести параметры виртуальной среды в соответствие требованиям PCI DSS, СТО БР ИББС, VMware Security Hardening Best Practice, CIS VMware ESX Server 3.5 Benchmark с помощью типовых политик безопасности

vGate содержит инструменты для обеспечения полноценной защиты гипервизора и средств управления виртуальной инфраструктурой от утечки информации по каналам, специфичным для виртуальной среды. Защиту от НСД к серверу виртуализации как внутри сети администрирования, так и от локального подключения можно организовать с помощью ряда настроек политик безопасности.

К таким настройкам относятся:

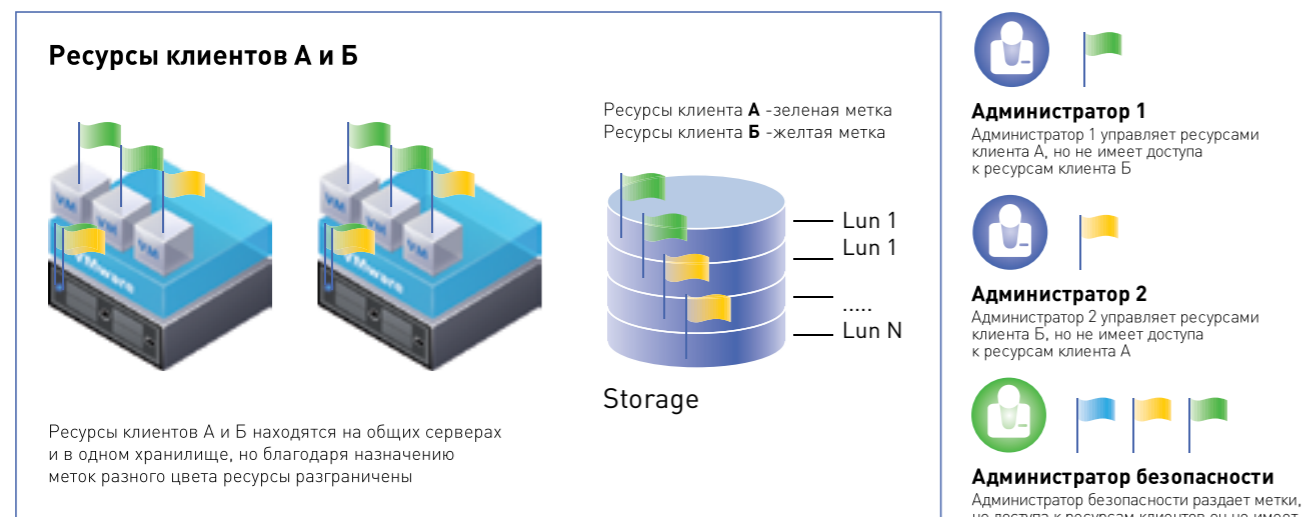
- список разрешенных для выполнения программ (доверенная программная среда сервера виртуализации);
- список запрещенных устройств (защита от несанкционированного копирования данных путем подключения внешних устройств);
- список пользователей, для которых разрешен локальный вход (защита от несанкционированного локального входа пользователей не из списка);
- запрет подключения USB-носителей (защита от несанкционированного копирования данных путем подключения USB-носителя);
- правила для брандмауэра (фильтрация трафика, поступающего на сервер виртуализации).

vGate обеспечит полноценную защиту гипервизора и средств управления виртуальной инфраструктурой от специфичных угроз виртуальной среды

Политики безопасности позволяют исключить возможность несанкционированного выноса и неконтролируемый рост числа VM благодаря таким настройкам, как управление возможностью создания снимков и клонирования VM, проверка целостности VM.

Для защиты от несанкционированного запуска программ до запуска ОС необходимо обеспечить доверенную загрузку сервера виртуализации. Для этого в каждый сервер рекомендуется установить плату доверенной загрузки, например ПАК «Соболь».

Защиту хранилищ данных с файлами VM от хищения или несанкционированного выноса можно обеспечить с помощью комплекса организационных мер (контроль доступа в помещения с хранилищами, опечатывание стоек и т. д.).



Для устранения беспокойства клиента о сохранности ресурсов можно регулярно предоставлять ему отчеты о состоянии настроек безопасности, соответствии политик безопасности отраслевым стандартам, а также отчеты об изменениях конфигурации и произошедших событиях информационной безопасности. vGate позволяет подготовить широкий набор различных отчетов по запросу или автоматически по расписанию. Например, можно

vGate позволяет подготовить отчеты:

- о состоянии настроек безопасности и соответствии политик безопасности отраслевым стандартам;
- об изменениях конфигурации и произошедших событиях информационной безопасности

ежемесячно отправлять клиенту отчет о соответствии политик безопасности требованиям стандарта PCI DSS. После несложной настройки vGate будет создавать такой отчет автоматически на фирменном бланке с логотипом клиента.

Клиентам, использующим бухгалтерские и финансовые программы, системы управления предприятием и персоналом и другие программы, обрабатывающие персональные данные, необходимо обеспечить соответствие ФЗ-152 «О персональных данных». vGate имеет сертификат ФСТЭК и позволяет защитить ИСПДн до класса К1 включительно.

vGate — сертифицированная защита ИСПДн до класса К1 включительно

Коротко о vGate R2

vGate — это сертифицированное средство защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальной инфраструктуры на базе платформ VMware Infrastructure 3 и VMware vSphere 4.

Функциональные возможности

- Защита информации от утечек через специфические каналы среды виртуализации.
- Разделение объектов инфраструктуры на логические группы и сферы администрирования через мандатное и ролевое управление доступом.
- Усиленная аутентификация, разделение ролей и делегирование полномочий.
- Управление и контроль над конфигурацией системы безопасности.
- Автоматическое приведение инфраструктуры в соответствие требованиям и постоянный контроль соответствия.

Соответствие требованиям

- PCI DSS.
- ФЗ-152 (РД ФСТЭК).
- СТО БР ИББС.
- VMware Security Hardening Best Practice.
- CIS VMware ESX Server 3.5 Benchmark.

- Мониторинг событий информационной безопасности (в том числе регистрация событий информационной безопасности, которые не регистрируются средствами vSphere).
- Создание отчетов о состоянии параметров безопасности виртуальной инфраструктуры, о произошедших событиях и внесенных в конфигурацию изменениях.

О компании

«Код Безопасности» — российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, конфиденциальных данных в среде виртуализации.

Высокое качество продуктов компании подтверждают сертификаты ФСТЭК, ФСБ и Министерства обороны России, что позволяет использовать средства защиты информации «Кода Безопасности» в организациях, где обрабатывается информация ограниченного доступа.

Компания «Код Безопасности» основана в 2008 году и входит в группу компаний «Информзащита» — признанного лидера в сфере информационной безопасности на российском рынке, является правопреемником ее многолетних исследований в области создания средств защиты информации для государственных и коммерческих заказчиков.

ЗАКАЗЧИКИ

Более 2500 государственных и коммерческих организаций в России доверяют продуктам компании «Код Безопасности» обеспечение безопасности своих информационных систем.

Крупные проекты, в которых используются продукты компании:

- подсистема информационной безопасности ГАС «Выборы»;
- защищенная телекоммуникационная система взаимодействия региональных подразделений Министерства финансов;
- защита информационных систем региональных управлений Банка России;
- подсистемы информационной безопасности Федерального казначейства, Федеральной таможенной службы, ОАО «ВымпелКом», концерна «Росэнергоатом».

ПАРТНЕРЫ

Более 400 авторизованных партнеров «Кода Безопасности» поставляют продукты и поддержку компании в 70 российских регионах.

ЛИЦЕНЗИИ

«Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России, ФСБ России и Министерства обороны.

ТЕХНОЛОГИЧЕСКИЕ АЛЬЯНСЫ

«Код Безопасности» стремится соответствовать высоким стандартам качества и инноваций при разработке новых программных средств защиты и является технологическим партнером ряда ведущих международных компаний — лидеров мирового рынка программного обеспечения и оборудования.

vmware®
PARTNER
TECHNOLOGY
ALLIANCE

Microsoft®
GOLD CERTIFIED
Partner

ISV/Software Solutions
Security Solutions

CITRIX®

Контакты

Почтовый адрес: **127018, Россия, Москва, а/я 55**

Адрес офиса в Москве: **ул. Образцова, 38**

Адрес офиса в Санкт-Петербурге: **Свердловская наб., 44**

Телефон: **+7 (495) 980-2345** (многоканальный)

Факс: **+7 (495) 980-2345**

Запрос дополнительной информации о продуктах

info@securitycode.ru

По вопросам стоимости и покупки продуктов

sales@securitycode.ru

По вопросам партнерства и сотрудничества

info@securitycode.ru

РЕГИОНАЛЬНЫЕ ПРЕДСТАВИТЕЛИ

Дальневосточный федеральный округ

тел.: **+7 (914) 543-7291**

e-mail: **r.shapiro@securitycode.ru**

Северо-Западный Федеральный Округ

тел.: **8 (812) 955-9012, 8 (921) 955-9012**

e-mail: **a.lagutin@securitycode.ru**



Код безопасности

ГК «Информзащита»