Код безопасности
ГК «Информзащита»

Выполнение требований стандарта PCI DSS при использовании технологий виртуализации

декабрь 2010

Введение

Виртуализация – одна из наиболее перспективных технологий корпоративного сектора. Внедрение данной технологии позволяет сократить капитальные и эксплуатационные затраты за счет снижения расходов на оборудование (серверы и аппаратные средства защиты), экономии электроэнергии и площадей серверных помещений, а также за счет снижения человеческих ресурсов на администрирование серверов. Некоторые компании только раздумывают над перспективами внедрения виртуализации, другие уже оценили экономическую эффективность от перевода вычислительных ресурсов на виртуальную платформу. Согласно статистике, в России в число инноваторов в этой сфере в первую очередь вошли ряд крупных банков и другие компании финансовой сферы.

Поскольку одной из важных задач для большинства компаний финансовой сферы является нормативное соответствие требованиям стандарта PCI DSS, владельцев таких компаний не может не волновать вопрос – как с наименьшими затратами обеспечить нормативное соответствие стандарту PCI DSS при обработке данных платежных карт в виртуальной среде?

Особенности выполнения требований стандарта PCI DSS в виртуальной среде

Требования стандарта PCI DSS (Payment Card Industry Data Security Standard) предъявляются к средам, где происходят хранение, обработка или передача данных платежных карт, а также к системным компонентам таких сред.

Очевидно, что требования стандарта PCI DSS должны выполняться и в виртуальной среде. Согласно недавно вышедшей в свет новой версии стандарта, требования применимы и к системным компонентам, к которым также относятся «компоненты виртуализации, такие как виртуальные машины, виртуальные коммутаторы/роутеры, виртуальные модули, виртуальные приложения и гипервизоры».

Кроме того, при выполнении требований стандарта должны быть учтены все известные уязвимости и специфичные каналы утечки, присущие виртуальной среде. И в ряде требований стандарта PCI DSS прямо или косвенно указывается на это. В частности, согласно требованию 2.2 «должны быть разработаны стандарты конфигурирования для всех системных компонентов, учитывающие все известные уязвимости и рекомендации по обеспечению безопасности систем».

Гипервизор (составная часть сервера виртуализации) и средства управления виртуальной инфраструктурой, к сожалению, являются потенциальными каналами утечки, посредством которых нарушитель может получить доступ к обрабатываемым на виртуальных машинах (ВМ) данным. С помощью гипервизора или средств управления виртуальной инфраструктурой злоумышленник может перехватить потоки данных, идущие с виртуальных машин на устройства (HDD, принтер, USB, сеть, дискеты), или получить непосредственный доступ к дискам хранилища с файлами виртуальных машин. Причем злоумышленник может получить доступ к дискам хранилища, даже когда ВМ выключены или не работают, без участия программного обеспечения этих виртуальных машин. Кроме того, администраторы виртуальной инфраструктуры, обладающие широкими полномочиями по манипуляции с ВМ и их файлами (дублирование ВМ, получение доступа к хранилищу ВМ, просмотр и копирование файлов ВМ и т. д.), являются по сути суперпользователями. Очевидно, что наличие суперпользователя может негативно влиять на эффективность защиты виртуальной инфраструктуры.

> Требования стандарта PCI DSS должны выполняться для виртуальной среды в первую очередь в части требований к построению и поддержанию защищенной сети и реализации мер по строгому контролю доступа

Какие же именно требования стандарта важно выполнить для «компонентов виртуализации»? Ответ на этот вопрос проиллюстрирован в таблице «Выполнение требований стандарта PCI DSS». Таким образом, в первую очередь важно выполнить требования к построению и поддержанию защищенной сети администрирования виртуальной инфраструктуры и реализации мер по строгому контролю доступа к ней в целом и серверам виртуализации в частности (т.е. требований стандарта 1, 2, 7 и 8). Выполнение этих требований позволит уменьшить вероятность получения доступа к данным платежных карт злоумышленниками и суперпользователями.

Обеспечение безопасности с помощью vGate

Новый продукт vGate компании «Код Безопасности» позволит значительно облегчить процесс приведения виртуальной инфраструктуры в соответствие требованиям стандарта PCI DSS.

vGate позволяет задать оптимальные настройки безопасности, в частности более двух десятков различных параметров серверов виртуализации и ВМ, практически за несколько минут. Для этого достаточно применить к тем объектам, где осуществляется обработка данных платежных карт, стандартный шаблон политик безопасности, входящий в состав продукта vGate.

При настройке этих параметров «вручную» потребуется куда больше времени. Кроме того, предъявляются довольно серьезные требования к квалификации администратора (он должен не только иметь необходимые навыки и опыт для настройки серверов виртуализации, но и быть экспертом в области PCI DSS). После настройки параметров безопасности «вручную» не гарантирована их неизменность в силу человеческого фактора. Значит и по истечении какого-то времени после настройки нельзя уже точно утверждать, что требования стандарта PCI DSS выполняются. Проведение дополнительных периодических проверок ведет к дополнительным затратам. vGate же обеспечивает постоянный контроль конфигурации критически важных параметров безопасности, что гарантирует их неизменность. Таким образом, vGate позволяет существенно снизить затраты на приведение и поддержание соответствия требованиям стандарта PCI DSS.

Как правило, задача отдельного выполнения требований стандарта PCI DSS стоит редко. Зачастую компании стремятся выполнить требования сразу комплекса стандартов и норм. vGate позволяет выполнить не только технические требования по соответствию отраслевому стандарту безопасности PCI DSS, но и требования так называемых best practice: VMware Infrastructure 3 Security Hardening и CIS VMware ESX Server 3.5 Benchmark. Кроме того, продукт имеет сертификат ФСТЭК и может применяться для защиты информационных систем персональных данных (ИСПДн) до класса К1 включительно.

Стандарты по обеспечению информационной безопасности в банковской сфере периодически дополняются. Трудно представить, что еще несколько лет назад никто не слышал о ФЗ №152, тогда как сейчас выполнение его требований — одна из основных задач для любой компании. Поэтому важно осознавать необходимость не просто формального выполнения требований очередного стандарта, а построения комплексной системы безопасности, учитывающей специфичные угрозы и уязвимости. Именно такую защиту виртуальной инфраструктуры с учетом специфичных угроз и уязвимостей виртуальной среды позволяет обеспечить vGate.

Виртуальная инфраструктура

На одной из ВМ сервера обрабатываются данные платежных карт

На всех ВМ сервера обрабатываются данные платежных карт

Для данном сервере не обрабатываются данные платежных карт

Метка безопасности с шаблоном политик PCI DSS

Таблица

«Выполнение требований стандарта PCI DSS»

	Требование PCI DSS	Применимость vGate для выполнения требования
Построение и поддержание защищенной сети	1. Должны быть обеспечены разработка и управление конфигурацией межсетевых экранов в целях защиты данных платежных карт	+
Защита данных платежных карт	2. Не должны использоваться параметры безопасности и системные пароли, установленные производителем по умолчанию	+
	3. Должна быть обеспечена защита данных платежных карт при хранении	+
Реализация программы управления уязвимостями	4. Должно обеспечиваться шифрование данных платежных карт, передаваемых по сетям общего пользования	+
	5. Должно использоваться и регулярно обновляться антивирусное программное обеспечение	+
Реализация мер по строгому контролю доступа	6. Должна обеспечиваться безопасность при разработке и поддержке систем и приложений	+
Регулярный мониторинг и тестирование сетей	7. Доступ к данным платежных карт должен быть ограничен в соответствии со служебной необходимостью	+
	8. Каждому лицу, имеющему доступ к вычислительным ресурсам, должен быть назначен уникальный идентификатор	+
	9. Физический доступ к данным платежных карт должен быть ограничен	Орг. меры
	10. Должен отслеживаться и контролироваться любой доступ к сетевым ресурсам и данным платежных карт	+
	11. Должно выполняться регулярное тестирование систем и процессов обеспечения безопасности	Орг. меры
Поддержание политики информационной безопасности	12. Должна поддерживаться политика информационной безопасности, регламентирующая деятельность сотрудников и контрагентов	Орг. меры

Коротко о vGate

vGate — это средство защиты информации в виртуальной инфраструктуре, обеспечивающее управление доступом и изменениями параметров безопасности. Продукт может применяться для виртуальных инфраструктур, построенных на базе платформ VMware Infrastructure 3 и VMware vSphere 4.

Соответствие требованиям

- PCI DSS 1.2.
- ФЗ-152 (РД ФСТЭК).
- VMware Security Hardening Best Practice.
- CIS VMware ESX Server 3.5 Benchmark.

Функциональные возможности

- Усиленная аутентификация и разделение прав на управление виртуальной инфраструктурой и на управление безопасностью.
- Мандатное и ролевое управление доступом через разделение объектов виртуальной инфраструктуры на логические группы и сферы администрирования с помощью бизнес-категоризации.
- Политики безопасности, позволяющие привести виртуальную инфраструктуру в соответствие положениям отраслевых стандартов и лучших мировых практик (PCI DSS, VMware Security Hardening Best Practice, CIS VMware ESX Server 3.5 Benchmark).
- Защита от утечек через каналы, специфичные для виртуальной инфраструктуры (контроль виртуальных устройств, обеспечение доверенной загрузки ВМ и контроль доступа к элементам виртуальной инфраструктуры).
- Аудит и глубокий мониторинг событий информационной безопасности (в том числе событий, которые не регистрируются средствами vSphere).
- Отчетность о состоянии параметров безопасности виртуальной инфраструктуры, о произошедших событиях и внесенных в конфигурацию изменениях.

Автоматический мониторинг соответствия инфраструктуры стандарту PCI DSS

В продукт vGate включен бесплатный модуль vGate Compliance Checker, который позволяет провести анализ соотвествия виртуальной инфраструктуры требованиям PCI DSS, а также ребованиям best practices: CIS VMware ESX Server Benchmarks, VMware Security Hardening Best Practices.

Интерфейс vGate Compliance Checker разработан в едином стиле с продуктом vGate и отличается удобством и простотой для использования. ИТ-специалисту необходимо сделать не более четырех операций для того, чтобы проверить систему своей компании: запустить продукт, указать объекты для проверки, выбрать из списка стандарты, на соответствие которым необходимо провести проверку, и запустить проверку. В среднем скорость проверки соответствия систем, в которых присутствует до 3 ESX-серверов, занимает около 1 минуты.

vGate Compliance Checker является бесплатной утилитой и доступен для скачивания на сайте www.securitycode.ru даже тем пользователем, которые еще не используют продукт vGate в повседневной работе.

* Получение сертификата на версию vGate 2 с вышеописанным функционалом планируется в конце 2010 – начале 2011 года. В данный момент имеется сертификат ФСТЭК (СВТ 5, НДВ 4) на версию 1.0.

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

Требование 1

Должны быть обеспечены разработка и управление конфигурацией межсетевых экранов в целях защиты данных платежных карт

1.2. Должна быть реализована такая конфигурация МЭ, которая ограничивает возможность подключения недоверенных сетей к системным компонентам среды данных платежных карт	Сервер авторизации vGate является по своей сути межсетевым экраном, который ограничивает возможность подключения недоверенных сетей к среде администрирования виртуальной инфраструктуры. Доступ во внутреннюю сеть администрирования, где возможен доступ к файлам виртуальных машин, предоставляется только с компьютеров, где установлен агент аутентификации vGate (после прохождения процедуры аутентификации). Кроме того, vGate блокирует любой веб-трафик из сети виртуальных машин в сеть администрирования виртуальной инфраструктуры.

Требование 2

Не должны использоваться параметры безопасности и системные пароли, установленные производителем по умолчанию

2.1. До подключения системы к сети должны быть изменены параметры, заданные производителем по умолчанию (например, пароли, SNMP-строки), а также удалены неиспользуемые учетные записи	Посредством политик безопасности vGate изменяет и контролирует конфигурацию параметров серверов виртуализации, заданных производителем по умолчанию, таких как: • политики паролей; • пароль штатного загрузчика; • полномочия на файлы, содержащие пароли пользователей; • полномочия на доступ к конфигурационным файлам протокола SNMP.
2.2. Должны быть разработаны стандарты конфигурирования для всех системных компонентов, учитывающие все известные уязвимости и рекомендации по обеспечению безопасности систем	vGate позволяет обеспечить конфигурирование серверов виртуализации в соответствии с рекомендации производителя и лучшими мировыми практиками (CIS VMware ESX Server 3.5 Benchmark и VMware Infrastructure 3 Security Hardening).
2.2.3. Параметры безопасности систем должны быть настроены для предотвращения ненадлежащего использования	Для предотвращения ненадлежащего использования серверов виртуализации и ВМ политики безопасности vGate задают и поддерживают конфигурацию следующих настроек безопасности серверов виртуализации: • ограничение полномочий на файлы по умолчанию для демонов и учетной записи root; • запрет подключения к виртуальным машинам внешних устройств для предотвращения копирования данных с ВМ; • запрет подключения к серверам виртуализации внешних USB-устройств; • блокирование служебных сообщений со стороны виртуальных машин к серверу виртуализации для предотвращения избыточного трафика; • назначение отдельной дисковой партиции на каждый раздел корневой файловой системы (/, /boot, /tmp, /home, /swap, /var/core, /var/log или /var) для предотвращения нехватки места на рабочем разделе и, соответственно, отказа в обслуживании.
2.3. Должно выполняться шифрование любого неконсольного административного доступа. Для управления с помощью веб-интерфейса и другого неконсольного административного доступа должны использоваться такие технологии, как SSH, VPN или SSL/TLS	Любой неконсольный административный доступ к серверам виртуализации шифруется с использованием протокола SSH. При этом политиками безопасности vGate задаются оптимальные параметры безопасности работы (запрет доступа под учетной записью root, запрет пустых паролей и т. д.), а также использование второй версии протокола SSH, которая является более безопасной по сравнению с SSH-1. Протокол SSH-2 устойчив к атакам прослушивания трафика («снифинг»), а также атакам путем присоединения посередине (session hijacking)

Требование 7

Доступ к данным платежных карт должен быть ограничен в соответствии со служебной необходимостью

7.1. Доступ к системным компонентам и данным платежных карт должен быть предоставлен только тем сотрудникам, которым он необходим для выполнения их должностных обязанностей. Ограничение доступа включает следующие меры:	Доступ к настройкам серверов виртуализации и иных объектов виртуальной инфраструктуры предоставляется только тем сотрудникам, которым он необходим для выполнения их должностных обязанностей (администраторам ВИ и администраторам ИБ). При этом управление настройками безопасности доступно только администраторам ИБ, а администрирование серверов виртуализации и иных объектов ВИ только администраторам ВИ

7.1.1. Права привилегированных пользователей ограничены минимально достаточными полномочиями, необходимыми для выполнения их должностных обязанностей	В vGate реализована функция разделения ролей пользователей, позволяющая устранить проблему суперпользователя. Управление безопасностью закреплено за администратором безопасности, а управление виртуальной инфраструктурой — за администратором виртуальной инфраструктуры. Доступ администратора безопасности к виртуальной инфраструктуре ограничен, и возможность его самосанкционировать отсутствует. Права каждого администратора виртуальной инфраструктуры ограничены администратором безопасности минимально необходимыми полномочиями для выполнения его должностных обязанностей (например, предоставлен доступ только к необходимым серверам виртуализации, запрещена/разрешена возможность скачивания файлов виртуальных машин или создания назначенных заданий и т. д.). Помимо этого, права доступа к серверам виртуализации ограничиваются политиками безопасности vGate, включающими: • обязательную аутентификацию в однопользовательском режиме; • ограничение входа в систему под учетной записью root; • разделение сетей консоли управления и виртуальных машин; • доступ к серверу виртуализации по сети с ограниченного набора IP-адресов; • более строгие настройки ядра для повышения безопасности работы по протоколу IPv4 и уменьшения вероятности удачной атаки на ESX-сервер; • более строгие настройки работы виртуального коммутатора, запрещающие смешанный режим, смену MAC-адреса и несанкционированные передачи.
7.1.2. Назначение полномочий сотрудникам в системах выполняется в соответствии с должностью и выполняемыми функциями	vGate позволяет назначать полномочия администраторам виртуальной инфраструктуры в соответствии с должностью и выполняемыми функциями с помощью меток безопасности. Метки позволяют одновременно контролировать соответствие настроек необходимых серверов виртуализации стандарту PCI DSS и доступ к ним только тех администраторов, в рамки обязанностей которых входит их администрирование.
7.1.4. Использование автоматизированных систем контроля доступа	vGate является автоматизированной системой контроля доступа на основе ролей. Доступ администраторов ВИ к серверам виртуализации и иным объектам сети администрирования ВИ дополнительно контролируется механизмами дискреционного и мандатного управления доступом.
7.2. Для многопользовательских системных компонентов должна быть реализована система контроля доступа по принципу необходимого знания, запрещающий любой доступ, не разрешенный явно. Эта система должна включать следующие характеристики:	К серверам виртуализации и иным объектам сети администрирования ВИ, которые можно отнести к многопользовательским системным компонентам, запрещен любой доступ, не разрешенный явно. При этом контролируется не только доступ, но и разрешенные операции с объектами ВИ. Список доступных операций формируется на базе правил мандатного управления доступом и особых привилегий администраторов ВИ. Специфичные каналы и уязвимости виртуальной среды, через которые возможен не разрешенный явно доступ, закрывают политики безопасности vGate, которые обеспечивают: • запрет операций с буфером обмена для ВМ; • ограничение списка пользователей, которым разрешено выполнять назначенные задания (команды cron и at); • использование протокола CHAP для проверки подлинности при подключении iSCSI-устройств; • ограничение на использование привилегий учетной записи su (привилегии суперпользователя su разрешены только членам группы wheel).
7.2.1. Распространяется на все системные компоненты	Комплексная система контроля доступа на базе мандатного и дискреционного контроля доступа охватывает все системные компоненты ВИ: серверы виртуализации, ВМ, сетевую подсистему (на уровне физических сетевых адаптеров и VLAN), хранилища данных (на уровне LUN), средства управления ВИ и иные объекты внутри сети администрирования виртуальной инфраструктуры.
7.2.2. Назначает пользовательские полномочия в соответствии с должностью и выполняемыми функциями	Назначение полномочий администраторам ВИ осуществляется с помощью меток безопасности в соответствии с должностью и выполняемыми функциями.
7.2.3. По умолчанию запрещает любые виды доступа	vGate запрещает по умолчанию все виды доступа. Например, если для какого-либо администратора ВИ не заданы дискреционные правила доступа к серверу виртуализации, то для него запрещены любые виды доступа как к самому серверу, так и к его настройкам.

Требование 8

Каждому лицу, имеющему доступ к вычислительным ресурсам, должен быть назначен уникальный идентификатор

8.1. Каждому пользователю должен быть присвоен уникальный идентификатор до предоставления доступа к системным компонентам или данным платежных карт	Каждому администратору виртуальной инфраструктуры в vGate (как дополнение к идентификатору для доступа к серверу виртуализации) назначается уникальное имя (логин) для доступа к защищенной виртуальной среде. При этом в качестве механизма аутентификации используется пароль.
8.2. В дополнение к назначению уникального идентификатора для всех пользователей должен использоваться по крайней мере один из следующих механизмов аутентификации: - Пароль или кодовая фраза - Двухфакторная аутентификация (например, устройства аутентификации, смарт-карты, биометрия или открытые ключи)	vGate позволяет однозначно сопоставить идентификатор для доступа в защищенную виртуальную среду vGate идентификатору для доступа к серверу виртуализации, что обеспечивает усиленную двухступенчатую аутентификацию администратора ВИ.
8.4. Все пароли должны быть приведены к нечитаемому виду при передаче и хранении на всех системных компонентах с помощью алгоритмов надежной криптографии	Пароли администраторов виртуальной инфраструктуры для доступа в защищенную виртуальную среду vGate передаются с использованием протокола Kerberos, гарантирующего защиту от прослушивания и атак повторного воспроизведения.
8.5. Для учетных записей сотрудников и администраторов на всех системных компонентах должны обеспечиваться надежная аутентификация и управление паролями, как описано в нижеследующих пунктах:	vGate обеспечивает надежную аутентификацию и управление паролями администраторов ВИ при доступе в защищенную среду, а также при доступе к системным компонентам серверов виртуализации. При этом администратор ВИ проходит процедуру аутентификации дважды: с помощью агента аутентификации vGate при доступе в защищенную среду и на сервере виртуализации при непосредственном сетевом доступе к нему.
8.5.1. Должно контролироваться добавление, удаление и изменение пользовательских идентификаторов, учетных данных и других объектов идентификации	Добавление, удаление и изменение учетных данных администраторов ВИ фиксируется в журнале событий. Политиками безопасности vGate контролируется доступ к конфигурационным файлам служб, файлам системного журнала сервера виртуализации и файлам, содержащим пароли пользователей сервера виртуализации. Кроме того, ограничивается возможность удаления файлов из перезаписываемых каталогов и перезаписи файлов для всех пользователей, а также гарантируется отсутствие программ с setuid- или getuid-флагами.
8.5.2. Должна выполняться проверка подлинности пользователей перед сбросом их паролей	Перед сбросом или сменой пароля администратора виртуальной инфраструктуры или сервера виртуализации производится проверка подлинности учетной записи администратора (до смены или сброса пароля запрашивается старый пароль).
8.5.3. Первоначально пароли для каждого пользователя должны быть уникальными и изменяться сразу же после первого использования	vGate выполняет проверку уникальности пароля администраторов ВИ и (по умолчанию) предлагает администратору виртуальной инфраструктуры сменить свой пароль при первом сеансе работы в защищенном режиме.
8.5.8. Не должны использоваться групповые, разделяемые или встроенные учетные записи и пароли	В vGate не используются групповые или встроенные учетные записи и пароли. Механизм vGate, позволяющий однозначно сопоставить идентификатору vGate идентификатор для доступа к серверу виртуализации, гарантирует отсутствие разделяемых учетных записей. Использование групповых и встроенных учетных записей для доступа к серверу виртуализации контролируется политиками безопасности vGate
8.5.9. Пользовательские пароли должны изменяться по крайней мере каждые 90 дней	Еженедельная (каждые 7 дней) смена пароля на сервере виртуализации контролируется политикой безопасности vGate. Срок действия пароля администратора виртуальной инфраструктуры для доступа в защищенный режим по умолчанию 30 дней (контролируется парольной политикой vGate).
8.5.10. Длина паролей должна составлять не менее 7 символов	Длина паролей на сервере виртуализации не менее 8 символов (контролируется политикой безопасности vGate). Значение длины паролей администраторов виртуальной инфраструктуры для доступа в защищенный режим контролируется парольной политикой vGate.
8.5.11.Пароли должны содержать как цифры, так и буквы	Пароли на сервере виртуализации должны содержать не менее трех различных классов символов из следующих: цифры, прописные и строчные буквы, знаки (контролируется политикой безопасности vGate). Количество классов символов в паролях администраторов виртуальной инфраструктуры контролируется парольной политикой vGate.
8.5.12. Должно быть запрещено создание нового пароля, если он совпадает с любым из последних четырех ранее использованных паролей	Количество ранее использованных паролей, с которыми не должен совпадать новый пароль администраторов виртуальной инфраструктуры контролируется парольной политикой vGate.

Требование 10

Должен отслеживаться и контролироваться любой доступ к сетевым ресурсам и платежным картам

10.1 Должен быть реализован процесс, связывающий осуществление любого доступа к системным компонентам (в особенности доступа с использованием административных привилегий, таких как root) с каждым конкретным пользователем	Связывание любого доступа к системным компонентам сервера виртуализации и ВМ осуществляется за счет функции сопоставления учетной записи vGate учетной записи сервера виртуализации. Благодаря этому можно однозначно идентифицировать, какой именно администратор ВИ получил доступ к системным компонентам.
10.2 Для всех системных компонентов должна выполняться регистрация событий с целью восстановления:	Регистрация событий, связанных с безопасностью виртуальной среды, выполняется централизованно на сервере аутентификации vGate. Кроме того, на каждом сервере виртуализации локально ведутся журналы событий.
10.2.2. Всех действий, выполненных с использованием административных привилегий	В журнале событий vGate фиксируются события, выполненные с использованием административных привилегий, такие как установка компонентов контроля целостности или применение политик безопасности к ESX-серверу, создание или удаление ВМ, доступ к файлам ВМ и т. д.
10.2.4. Неудачных попыток логического доступа	В журнале событий vGate фиксируются факты неудачных попыток логического доступа, например, попытки доступа к файлам ВМ
10.2.5. Использования механизмов идентификации и аутентификации	В журнале событий vGate регистрируются события, связанные с аутентификацией администраторов и компьютеров, причем фиксируются как удачные, так и неудачные попытки аутентификации
10.2.7. Создания и удаления системных объектов	В журнале событий vGate регистрируются события создания и удаления системных объектов, например: • добавление или удаление серверов виртуализации из списка защищаемых; • добавление или удаление компонентов контроля целостности; • создание или удаление ВМ.
10.3. В регистрируемых событиях для каждого системного компонента должны записываться по крайней мере следующие элементы: 10.3.1. Идентификатор пользователя 10.3.2. Тип события 10.3.3. Дата и время 10.3.4.Индикатор успеха или отказа 10.3.5. Источник события 10.3.6. Идентификатор или название задействованных данных, системного компонента или ресурса	В событиях, регистрируемых в журнале vGate, фиксируются: • учетная запись пользователя в качестве идентификатора пользователя (п. 10.3.1); • тип события (п. 10.3.2); • дата и время события (п.10.3.3); • название компьютера в дополнение к идентификатору пользователя; • тип события (успех, уведомление, предупреждение, ошибка) в качестве индикатора успеха или отказа (п. 10.3.4); • код события; • компонент vGate, к которому относится событие (ESX-агент, vCenter, служба контроля целостности, служба удаленного управления и т. д.), в качестве источника события (п. 10.3.5); • категория событий (аутентификация, виртуальные машины, политики, управление доступом и т. д.) в качестве идентификатора или названия задействованных данных, системного компонента или ресурса (п. 10.3.6); • описание события.
10.4. Должна выполняться синхронизация времени на всех критичных системах	Синхронизация времени на сервере виртуализации по протоколу NTP управляется политикой vGate
10.7. Журналы регистрации событий должны храниться по крайней мере в течение 1 года, при этом в течение 3 месяцев журналы должны быть доступны в режиме оперативного доступа для анализа (например, в режиме онлайн, в виде архива или чтобы их можно было восстановить из резервной копии)	vGate задает следующие параметры хранения журналов для ВМ: • размер файла событий — 100000 байт; • размер архива — 10 файлов. vGate задает следующие параметры хранения журналов для серверов виртуализации: • использовать архивацию файлов; • размер файла событий — 2096 Кб. Как правило, вышеуказанные параметры ведения журналов гарантируют доступность событий (при средней частоте появления событий и типовом количестве ВМ на сервере виртуализации) по крайней мере в течение 1 года на сервере виртуализации и ВМ. Журнал событий на сервере авторизации хранится в БД PostgreSQL и ограничений на размер файлов не существует.

Код Безопасности
ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.
Адрес офиса в Москве: ул. Образцова, д. 38.
Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.
Тел.: +7 (495) 980-2345 (многоканальный).
Факс: +7 (495) 980-2345.
E-mail: info@securitycode.ru
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

Вы можете узнать подробную информацию о продуктах на сайте
www.securitycode.ru

О компании «Код Безопасности»

Компания «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, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.