ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**на оказание услуг по предоставлению и установке средства защиты информации vGate R2 Standard**

1. Общие сведения
	1. Наименование оказываемых услуг:

Услуги по предоставлению и установке средства защиты информации vGate R2 Standard

* 1. Состав услуг

Услуги включают:

* поставка средств защиты информации;
* поставка сертификата активации сервиса технической поддержки;
* установка средств защиты информации.
	1. Сроки (периоды) оказания услуг:

Срок оказания услуг должен составлять не более 30 (тридцати) рабочих дней с даты заключения контракта

1. Требования к услуге:

Все компоненты СЗИ должны соответствовать или превышать показатели и требования, указанные в Приложениях № 1 и № 2 к настоящему Техническому заданию.

Качество поставляемых СЗИ должно соответствовать государственным стандартам качества, техническим условиям и иметь все необходимые сертификаты.

Все поставляемые компоненты СЗИ должны быть полностью совместимы между собой.

Сертификат активации сервиса технической поддержки предоставляет пользователю право на получение услуг в целях обеспечения качественного, устойчивого и бесперебойного функционирования поставляемого оборудования.

Установка и настройка поставляемых средств защиты информации должна быть произведена по отдельному списку, согласно Приложению № 3 к настоящему Техническому заданию, в соответствии с предоставленной Заказчиком проектной документацией, в которой будут отражена вся необходимая для настройки информация.

При установке и настройке поставляемых средств защиты информации Поставщик обязан обеспечить конфиденциальность полученной информации о структуре системы защиты, ключевых материалах и т.п.

1. Лицензионные требования к Исполнителю

Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на следующие виды работ:

* установка, монтаж, наладка, испытания, ремонт средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).
1. Требования к документации

Все средств защиты информации должны поставляться с комплектом технической документации и руководством пользователя.

Все необходимые руководства пользователя и техническая документация должны быть на русском языке.

1. Гарантийное обслуживание

Все поставляемые в рамках услуг средства защиты информации должны быть обеспечены гарантийным обслуживанием в течение срока, установленного Поставщиком, но не менее одного года с момента принятия их Заказчиком.

1. Состав, количество и характеристики поставляемого оборудования и объем оказываемых услуг(Спецификация)

Необходимое количество, требования к поставляемым средств защиты информации, услугам, характеристики приведены в Приложении № 1 и №2 к Техническому заданию.

Перечень мест для установки средств защиты информации приведен в Приложении № 3 к настоящему Техническому заданию.

Приложение № 1

к Техническому заданию

Количество поставляемых средств защиты информации

| **№****п/п** | **Наименование**  | **Объем**  |
| --- | --- | --- |
| **Единица****измерения** | **Кол-во** |
|  | Право на использование Средства защиты информации vGate R2 Standard (за 1 физический процессор на защищаемом хосте)Страна происхождения –Россия(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | лицензия | 2 |
|  | Ключ активации сервиса совместной технической поддержки уровня "Стандартный" для СЗИ vGate R2Страна происхождения –Россия(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | шт. | 2 |

Приложение № 2

к Техническому заданию

Технические требования к поставляемым средствам защиты информации

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Наименование** | **Требования** |
| 1 | Право на использование Средства защиты информации vGate R2 Standard (за 1 физический процессор на защищаемом хосте)Страна происхождения –Россия(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | ***Требования к поддержке платформ виртуализации:**** VMware vSphere 6.5;
* VMware vSphere 6.7;
* VMware vSphere 7.0;
* Ubuntu 18.04.6 LTS;
* Ubuntu 20.04.3 LTS;
* Astra Linux Common Edition "Орел" 2.12.22;
* Альт Сервер Виртуализации 10;
* Альт Сервер 8 СП.
* Скала-Р Управление 1.80;
* Скала-Р Управление 1.93;
* OpenNebula 5.10.5, Proxmox 7.0 в составе Альт Сервер Виртуализации 10;
* Proxmox 7.2.

***Должно осуществлять:*** * аутентификацию администраторов виртуальной инфраструктуры и администраторов безопасности;
* защиту средств управления виртуальной инфраструктурой от НСД;
* защиту серверов виртуализации (гипервизоров) от НСД;
* контроль целостности конфигурации виртуальных машин и их доверенную загрузку;
* затирание остаточных данных на СХД при удалении виртуальной машины;
* мандатный принцип контроля доступа;
* регистрацию событий, связанных с информационной безопасностью;
* контроль целостности и защиту от НСД компонентов СЗИ;
* централизованное управление и мониторинг;
* создание резервной копии конфигурации СЗИ и журналов аудита.

 ***Требования к функциональности:***- **Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности** В СЗИ должна быть реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью (для ограничения на использование привилегий суперпользователя). Должна быть возможность выделить 2 основные роли — администратор виртуальной инфраструктуры и администратор безопасности. В рамках роли администратора виртуальной инфраструктуры должна быть возможность разграничения доступа по привилегиям\типам объектов доступа. Должна быть поддержка аппаратных идентификаторов JaCarta и RuToken.*Реализация принципа разделения ролей*Доступ на управление виртуальной инфраструктурой или параметрами безопасности должен предоставляться только для аутентифицированных пользователей. Для этого в СЗИ должна быть предусмотрена процедура аутентификации пользователей и компьютеров (рабочих мест администраторов), которая должна осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа Man in the Middle.Процедура аутентификации должна осуществляется с помощью отдельной программы, которую требуется запустить и ввести учетные данные до того, как осуществляется соединение с виртуальной инфраструктурой.Функционал аутентификации на рабочем месте администратора должен предоставлять возможность надежно сохранить учетные данные. СЗИ должно иметь собственную систему учетных записей или иметь возможность интегрироваться с Microsoft Active Directory.СЗИ должно поддерживать работу администраторов виртуальной инфраструктуры через Web-интерфейс, интерфейс командной строки (VMware PowerCLI) а также через ESXi Embedded Host Client.СЗИ должно иметь возможность отключения механизмов защиты в аварийных ситуациях и в режиме тестирования.СЗИ должно иметь возможность экспорта\импорта настроек конфигурации.СЗИ должно иметь возможность аутентификации администраторов без установки дополнительного ПО на рабочем месте (посредством Web-интерфейса)СЗИ должно оповещать пользователя после аутентификации о дате и времени его последнего входа в системуСЗИ должно иметь возможность блокировать параллельные сеансы администраторов виртуальной инфраструктуры**- Защита средств управления виртуальной инфраструктурой от НСД**К средствам управления виртуальной инфраструктурой относятся:* ESXi-хосты, предназначенные для запуска виртуальных машин;
* серверы vCenter, предназначенные для централизованного управления виртуальной инфраструктурой;
* серверы vSphere Web Client, предназначенные для поддержки управления виртуальной инфраструктурой через «тонкий» клиент;
* средства, предназначенные для обслуживания инфраструктуры, например, VMware Consolidated Backup, VMware Update Manager;
* сторонние средства мониторинга и управления инфраструктурой.
* KVM-серверы, предназначенные для запуска виртуальных машин.
* СУПВ Скала-Р Управление
* Сервер Proxmox
* Сервер OpenNebula

Для обеспечения защиты средств управления виртуальной инфраструктурой должен применяется функционал мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Для этого весь управляющий трафик должен проходить через компонент СЗИ, осуществляющий этот контроль. Правила разграничения доступа должны работать на основе меток и уровней безопасности, а также заданных ACL и параметров соединения (протоколов, портов). Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами должен подписываться, для обеспечения защиты от атак типа Man in the Middle в процессе сетевого взаимодействия.В СЗИ должен присутствовать механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым должна обеспечивается защита средств управления виртуальной инфраструктурой от НСД со стороны скомпрометированной виртуальной машины.В СЗИ должна быть предусмотрена возможность ограничения миграции виртуальных машин за пределы управления текущего vCenter;В СЗИ должен присутствовать оповещения администратора виртуальной инфраструктуры о том, что действие заблокировано СЗИ.В СЗИ должен присутствовать механизм контроля операций VMware vCenter без необходимости установки на него агента защиты.**- Защита серверов виртуализации (гипервизоров) от НСД**В рамках обеспечения защиты ESXi-хостов от НСД в СЗИ должны быть реализованы следующие механизмы:* возможность создания списка разрешенных программ;
* возможность контроля разграничения сети управления и сети виртуальных машин;
* возможность настройки параметров логирования виртуальных машин;
* возможность создания списков запрещенных устройств;
* возможность отключения VIX API;
* возможность запрета коммуникаций между виртуальными машинами;
* возможность ограничения объема VMX-файла;
* возможность контроля за использованием independent-nonpersistent дисков;
* возможность проверки использования стандартных SSL сертификатов;
* возможность запрета использования Managed Object Browser;
* возможность отключения приветственной страницы;
* возможность контроля VMsafe;
* возможность создания списка пользователей, которым разрешен локальный вход на ESXi-сервер;
* возможность запретить сжатие виртуального диска;
* возможность ограничения количества активный консольных подключений;
* возможность блокирования подключения USB-носителей к ESXi-серверу;
* возможность осуществления контроля и настройки правил встроенного межсетевого экрана;
* возможность запрета клонирования и создания снимков виртуальных машин;
* возможность очистки внешней и оперативной памяти при окончании работы с виртуальной машиной;
* возможность ограничения доступа к конфигурационным файлам служб;
* возможность запрета непосредственного доступа к управлению ESXi-сервера;
* возможность контроля использования протокола SSH;
* возможность запрета операций с буфером обмена для каждой виртуальной машины;
* возможность контроля использования CHAP для проверки подлинности при подключении iSCSI-устройств;
* возможность создания парольных политик;
* возможность отключения неиспользуемых протоколов, портов и функций;
* возможность настройки безопасности виртуального коммутатора;
* запрет использования VMware Tools;
* запрет возможностей, не реализованных в vCenter;
* возможность запрета контроля устройств ESXi-сервера со стороны виртуальных машин;
* возможность запрета отсылки информации о производительности ESXi-сервера гостевым системам;
* возможность настройки синхронизации времени;
* возможность на запрет доступа консоли виртуальной машины.

В рамках обеспечения защиты KVM-серверов виртуализации от НСД в СЗИ должен применяется функционал мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Для этого весь управляющий трафик должен проходить через компонент СЗИ, осуществляющий этот контроль. Правила разграничения доступа должны работать на основе меток и уровней безопасности, а также заданных ACL и параметров соединения (протоколов, портов). **- Контроль целостности конфигурации виртуальных машин и доверенная загрузка**СЗИ должно содержать компоненты, устанавливаемые на каждый сервер виртуализации (гипервизор) и реализующие следующие механизмы защиты:Для ESXi-хостов:* Контроль целостности настроек виртуальной машины перед ее загрузкой. Должен контролироваться файл \*.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров.
* Контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ должно контролировать целостность файла \*.nvram, в котором содержится образ BIOS виртуальной машины.
* Доверенная загрузка ОС должна осуществляться путем контроля целостности загрузочного сектора виртуального диска \*.vmdk.
* Контроль целостности шаблонов виртуальных машин, включая виртуальные жесткие диски.

Для KVM-хостов:* Контроль целостности настроек виртуальной машины перед ее загрузкой. Должен контролироваться файл конфигурации, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров.

При изменении одного из перечисленных объектов как санкционированном, так и несанкционированном, СЗИ должно предоставить администратору безопасности возможность данные изменения принять или отменить (для ESXi-хостов). **- Мандатный принцип контроля доступа**В СЗИ должен быть реализован мандатный принцип контроля доступа на основе меток конфиденциальности. Должно присутствовать два вида меток конфиденциальности: иерархические (далее просто метки) и неиерархические (далее просто категории). Должна быть реализована возможность назначить метки на следующие субъекты, объекты, контейнеры:* Администраторы ВИ;
* ESXi-хосты;
* Сетевые адаптеры ESXi-хоста;
* Виртуальные сети;
* Разделы хранилищ (Datastore);
* Виртуальные машины;
* Серверы управления;
* Группы объектов;
* KVM-серверы.

Права доступа субъектов и объектов должны проверяться на основе меток и категорий автоматически и запрещать несанкционированные действия. Субъект может получить доступ к объекту, только если выполняется условие соответствия их меток конфиденциальности. Для категорий – это совпадение хотя бы одной из категорий субъекта и объекта, для меток – это уровень иерархии субъекта должен быть равен (или выше, в зависимости от настроек СЗИ) уровню объекта.Категории должны отличаться от меток следующими параметрами:* Метки должны быть иерархическими, категории равноправными.
* Механизмы работы меток должны зависеть не только от пользователя, но и от его меток его текущей сессии. Категории от сессии зависеть не должны.
* Любой субъект, объект, контейнер может быть помечен несколькими категориями и только одной меткой.

Должен быть предусмотрен механизм отключения контроля мандатного доступа по типам объектовДолжен быть предусмотрим механизм автоматизированного добавления виртуальных машин в группы объектов.**- Регистрация событий, связанных с информационной безопасностью** В СЗИ должен быть реализован механизм регистрации следующих групп событий:* События аутентификации и разграничения доступа;
* Средство должно регистрировать как удачные, так и неудачные попытки доступа к инфраструктуре (с указанием имени учетной записи, даты, имени компьютера или его IP-адреса)
* Средство должно регистрировать события изменений конфигурации параметров безопасности и учетных записей администраторов инфраструктуры
* События контроля целостности СЗИ, контроля целостности и доверенной загрузки виртуальных машин;
* События, связанные с установкой, удалением, включением, остановом и сбоем компонентов СЗИ, а также с изменением настроек СЗИ.

Регистрация событий на всех компонентах СЗИ должна осуществляется в едином журнале. Для всех групп событий должны регистрироваться как факты НСД, так и правомочные действия.Должна быть возможность отбора событий безопасности по типу, дате и времени события, объекту\субъекту доступа.В СЗИ должен быть реализован механизм отправки уведомлений о событиях безопасности по протоколам SMTP и Syslog. **- Контроль целостности и защита от НСД компонентов СЗИ** СЗИ должен содержать собственные механизмы контроля целостности компонентов СЗИ. Механизмы должны действовать на всех компонентах СЗИ.- **Централизованное управление и мониторинг** СЗИ должно содержать Консоль управления, устанавливающуюся на рабочее место администратора безопасности со следующим функционалом:* управление учетными записями администраторов виртуальной инфраструктуры и администраторов безопасности;
* назначение прав на доступ к защищаемым объектам;
* развертывание и настройка компонентов защиты ESXi-хостов;
* настройка правил разграничения запуска виртуальных машин и утверждение изменений параметров виртуальных машин, произведенных администраторами ВИ;
* просмотр журнала регистрации событий безопасности.

Все изменения, произведенные администратором безопасности, должны сохраняться централизованно.**- Создание резервной копии конфигурации СЗИ и журналов аудита**СЗИ должно иметь возможность экспорта собственной конфигурации в указываемую директорию и импорта конфигурации из данного файла. Должа быть возможность настройки выгрузки журналов аудита по достижению заданного размера базы или по сроку хранения событий.***Требования по сертификации:***СЗИ должно иметь действующий сертификат ФСТЭК России и соответствовать требованиям по безопасности информации установленным в документах:* «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по классу защищенности не ниже 5-го;
* «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» по уровню доверия не ниже 4-го.
 |
| 2 | Ключ активации сервиса совместной технической поддержки уровня "Стандартный" для СЗИ vGate R2Страна происхождения –Россия(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | **Требования к сертификатам активации сервиса совместной технической поддержки**1. Сертификат активации сервиса совместной технической поддержки должен поставляться на бумажном носителе, выпущенном производителем - ООО «Код безопасности», сроком действия не менее 1 года.
2. Техническая поддержка работоспособности средств защиты информации должна осуществляться в течение срока действия сертификата.
3. Сертификат активации сервиса совместной технической поддержки должен предоставлять возможность обращаться в техническую поддержку Исполнителя по вопросам:
* консультации работников Заказчика по электронной почте;
* получения обновления программного обеспечения при выходе новых и исправленных версий.

Техническая поддержка должна быть оказана в соответствии с условиями, указанными на сайте производителя: <https://www.securitycode.ru/>  |

Приложение № 3

к Техническому заданию

**Перечень мест для установки средств защиты информации**

| **№****п/п** | **Наименование учреждения** | **Адрес****установки** | **Количество** |
| --- | --- | --- | --- |
| 1 |  |  | 1 |