**ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ**

**Приобретение системы управления средой виртуализации Роса:** Поставка лицензии системы управления средой виртуализации «Rosa –virtualization» сертифицированной ФСТЭК

1. Общие сведения
	1. Предмет закупки: Приобретение системы управления средой виртуализации Роса: Поставка лицензии системы управления средой виртуализации «Rosa –virtualization» сертифицированной ФСТЭК.

Заказчиком при описании объекта закупки не применяются слова «или эквивалент» в соответствии с пунктом 1 части 1 статьи 33 Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения совместимости с программным обеспечением, правами на использование которого уже владеет Заказчик (Контракт бюджетного учреждения №0162200011824001186 от 06.05.2024) Иное программное обеспечение не обеспечит совместимости с уже эксплуатируемым программным обеспечением, что повлечет дополнительные расходы и ресурсы на интеграцию эквивалентного программного обеспечения.

Наименование объекта закупки и количественные показатели:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование услуги | Единица измерения | Количество |
|  | Поставка лицензии системы управления средой виртуализации «Rosa –virtualization» сертифицированную ФСТЭК; | штука | 33 |

* 1. Заказчик: ГБУ СО «Оператор электронного правительства».
	2. Место поставки программного обеспечения, передачи прав, внедрения: г. Екатеринбург, ул. Большакова, 105 - ГБУ СО «Оператор электронного правительства»
	3. Срок поставки ПО, передачи прав, выполнения работ: в течение 30 календарных дней с даты заключения Контракта.
	4. Код позиции по ОКПД2: 58.29.5 (Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение).

Код позиции по КТРУ: 58.29.50.000-00000001 (Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение).

Передаваемые права на программное обеспечение должны быть свободны от любых прав третьих лиц, не находиться под запретом (арестом), в залоге и не являться предметом спора третьих лиц.

* 1. Цель и задачи оказания услуг:

 - осуществление полного перехода на российскую платформу виртуализации, сертифицированную ФСТЭК:

* + Миграция серверов системы виртуализации на ПО виртуализации сертифицированную ФСТЭК;
	+ Обеспечение отказоустойчивой работы виртуальных машин в процессе модернизации виртуальной инфраструктуры Заказчика.
	+ Формирование документации по виртуальной инфраструктуре.
	1. Состав услуг:
	+ Предоставление прав использования прав использования системы управления средой виртуализации;
	+ Внедрение системы виртуализации:
	+ Формирование документации по виртуальной инфраструктуре.
	1. Способ поставки (передачи):

ПО должно быть поставлено (передано) следующим способом:

Дистрибутив ПО:

* на компакт-диске (DVD, CD) с дистрибутивами экземпляров ПО включая формуляр ФСТЭК.

Ключ активации ПО (лицензионный ключ):

* в виде отдельного файла на компакт-диске с дистрибутивом ПО, либо в виде электронного файла на адрес электронной почты Заказчика, указанной в Контракте.

Ссылка для скачивания дистрибутива ПО с сайта разработчика (правообладателя) должна быть активна и позволять скачать дистрибутивы ПО без дополнительной авторизации и оплаты в объеме, установленном в настоящем Описании объекта закупки.

1. Перечень сокращений, термины и определения

| Наименование | Расшифровка |
| --- | --- |
| ГОСТ | Государственный стандарт |
| ЛВС | Локальная вычислительная сеть |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| СХД | Система хранения данных |
| ТЗ | Техническое задание |
| ФЗ | Федеральный закон |
| ТЗ | Техническое задание |
| ЗИП | Запасные части, инструменты и принадлежности |

1. Требования к Услугам

Заказчиком при описании объекта закупки не применяются слова «или эквивалент» в соответствии с пунктом 1 части 1 статьи 33 Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения совместимости с программным обеспечением, правами на использование которого уже владеет Заказчик. Иное программное обеспечение не обеспечит совместимости с уже включенным программным обеспечением, что повлечет дополнительные расходы и ресурсы на интеграцию эквивалентного программного обеспечения.

Программное обеспечение должно быть в комплекте: 33 шт. – передача неисключительных прав на сертифицированную систему управления средой виртуализации на 1 хост (до 2 ЦПУ), 1 шт.- медиа-комплект для сертифицированной системы управления средой виртуализации.

Срок действия неисключительных прав - бессрочно.

* + 1. Общие требования

Системы управления средой виртуализации должна быть внесена в единый реестр программного обеспечения для электронных вычислительных машин и баз данных Минкомсвязи;

Разработчик должен иметь собственную платформу разработки полного цикла, зарегистрированную и находящуюся на территории РФ;

Система управления средой виртуализации должна обладать русскоязычным интерфейсом;

Система управления средой виртуализации должна обладать централизованным механизмом управления виртуализацией с графической консолью администрирования и управления виртуальными машинами, шаблонами, рабочими столами, хранилищами, кластерами и центрами обработки данных;

Система управления средой виртуализации должна иметь набор инструментов для переноса ВМ из других систем виртуализации, в том числе VMWare vSphere;

Система управления средой виртуализации должна обладать высокой масштабируемостью хоста и гостевых ВМ;

Может использоваться:

* в государственных информационных системах 1-го класса защищенности в соответствии с документом "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", утвержденным приказом ФСТЭК России от 11 февраля 2013 года №17;
* в информационных системах персональных данных 1-го уровня защищенности в соответствии с документом "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденным приказом ФСТЭК России от 18 февраля 2013 года №21.
	+ 1. Функционально-технические требования

Системные требования и ограничения.

|  |  |  |
| --- | --- | --- |
| № | Функционал | Требования к функционалу |
| 1 | Создание и управление виртуальными средами с возможностью обеспечения высокой доступности виртуального сервера в случае сбоя физического сервера (кластеризация) | Поддержка функций высокой доступности:кластеризация хост-серверов с автоматическим восстановлением работы виртуальных машин в случае выхода из строя одного или нескольких хост-северов кластера; |
| Наличие режима высокой доступности для центра управления системой виртуализации. |
| Возможность использовать политики для автоматической балансировки нагрузки между хостами кластера. |
| Возможность создания профиля узлов |
| Возможность автоматизации развертывания узлов |
| Централизованное управление кластером и несколькими кластерами, входящими в состав ЦОД; |
| Режим высокой доступности контроллера домена; |
| создание кластеров, состоящих не менее чем из 64 узлов; |
| создание кластеров, с возможностью расширения количества управляемых ВМ до значения не менее чем из 8000 ВМ; |
| автоматическая балансировка нагрузки ЦП между узлами кластера (DRS); |
| возможность перезапуска критически важных ВМ на другом хосте в случае сбоя оборудования с тремя уровнями приоритета и с учётом политики отказоустойчивости. |
| размещение виртуальных машин на хосте на основе правил совместного и несовместного размещения (DRS Host Affinity Rules); |
| возможность запретить размещение виртуальных узлов кластера на одних и тех же физических серверах платформы виртуализации, серверах, установленных в одну стойку (виртуальную машину можно привязать к хосту или кластеру стойки); |
| выравнивание инструкций ЦП на всех узлах кластера (nodes) под минимально совместимый набор инструкций (EVC); |
| создание виртуальных машин на основе предустановленных шаблонов; |
| создание виртуальных машин на основе технологии клонирования; |
| автоматическое управление питанием (DPM) для автоматического выключения серверов при снижении нагрузки; |
| 2 | Создание и управление виртуальными средами с поддержкой перемещения виртуальных машин | возможность перемещения виртуальных машин с одного хоста на другой без прерывания их работы; |
| возможность использовать режим обслуживания хоста, позволяющий автоматически переносить запущенные виртуальные машины на другой хост и проводить обновление гипервизора или оборудования. |
| возможность перемещения файлов виртуальных машин между хранилищами без прерывания работы ВМ; |
| 3 | Количество запущенных виртуальных машин на хост | Не менее 100, если позволяют аппаратные ресурсы хоста |
| 4 | Создание и управление виртуальными средами с поддержкой катастрофоустойчивости (репликации ВМ): | Возможность репликации виртуальных машин со следующими параметрами репликации (в ручном режиме):RPO — от 15 минут до 24 часов;возможность установки параметров на уровне ВМ |
| 5 | Управление ресурсами виртуальной инфраструктуры | Централизованное управление всеми ресурсами управляемой инфраструктуры, включая управление хост-серверами, LAN, СХД и распределенными коммутаторами |
| 6 | Возможность резервного копирования основных компонентов системы виртуализации (гипервизора, системы управления, ВМ, виртуальных сетевых устройств, виртуального оборудования) | Централизованное выполнение полных резервных копий виртуальных машин встроенными средствами системы виртуализации в ручном или автоматическом режиме по расписанию, без необходимости установки агентов в гостевых ОС и без загрузки сети передачи данных (LAN) при условии выполнения задач напрямую в SAN. Возможность создания резервных копий текущего состояния ВМ в составе:- Настроек ВМ;- Дисковой подсистемы;- Оперативной памяти. |
| 7 | Возможность выполнения резервного копирования с помощью ПО третьих фирм | Возможность выполнения бэкапа данных из гостевых ВМ программными решениями третьих фирм при наличии драйвера ShadowCopy. Эксплуатационная совместимость с ПО для резервного копирования Acronis и Bacula |
| 8 | Поддержка технологии ускоренного инкрементального бэкапа (CBT) | Ускоренное выполнение инкрементального бэкапа за счёт анализа изменившихся блоков с использованием ПО Acronis и Bacula |

* + 1. Требования к инструментам администрирования и управления

|  |  |
| --- | --- |
| № | Требования к управлению |
| 1 | Наличие системы установки обновлений для компонентов гипервизоров |
| 2 | Поддержка функциональности SSO для компонентов системы и разделения уровней доступа на основе ролевой модели |
| 3 | Наличие интерфейсов SSH, CLI и WEB для управления системами виртуализации |
| 4 | Возможность сбора и анализа логов всей используемой инфраструктуры, консолидации журналов компонентов виртуализации для сопоставления и корреляции (с использованием syslog) |
| 5 | Наличие доступа к консоли виртуальной машины из системы управления гипервизором с возможностью подключения физических и логических локальных устройств, и носителей (USB, ISO, приводов CD/DVD) на «лету» |
| 6 | Возможность мониторинга по протоколу SNMP всех компонентов виртуальной инфраструктуры |
| 7 | Возможность экспорта данных syslog для анализа причин отказов оборудования |
| 8 | Унифицированное и автоматизированное конфигурирование хоста из сохраненных конфигураций на базе политик и профилей (единый шаблон рабочей конфигурации) |

* + 1. Требования к функциональным характеристикам

|  |  |  |
| --- | --- | --- |
| № | Функционал | Требования к функционалу |
| 1 | Создание и управление виртуальными средами с заданной конфигурацией виртуальных машин | Параметры виртуальных машин:до 128 виртуальных ЦП (эксплуатационно протестирована работа 128 vCPU);до 2 ТБ RAM;жёсткий диск объёмом до 10 ТБ (минимум 25 ГБ, рекомендуется от 50 ГБ) |
| - возможность администраторам выделять виртуальным машинам больше ОЗУ, чем присутствует на физическом хосте; |
| * поддержка 32- и 64-битных виртуальных машин и симметричной мультипроцессорной обработки внутри ВМ;
 |
| * поддержка возможности доступа из виртуальной машины к USB-устройствам, подключенным к хосту;
 |
| * поддержка возможности проброса физических устройств хранения (LUN) в виртуальную машину;
 |
| * мониторинг производительности виртуальных машин на основе метрик производительности;
 |
| * возможность лимитировать загрузки по ЦП для виртуальных машин
 |
| 2 | Создание и управление виртуальными средами с заданной конфигурацией хостов: | Параметры хостов (гипервизоров):* возможность загрузки гипервизора с USB-накопителя;
 |
| * возможность управления виртуальными ресурсами со следующими параметрами (на хост):
* размер слоя гипервизора на СХД — 1,5 ГБ;
 |
| * возможность управления виртуальными ресурсами со следующими параметрами (на хост):
* до 480 vCPU. Поддерживаются серверы архитектуры Intel x86-64 с конфигурацией до 160 логических процессоров, имеющих до 2 ТБ ОЗУ каждый. Эксплуатационно протестирована возможность функционирования комплекса с двукратным превышением параметров логических процессоров и количества задействованных процессоров в ВМ;
 |
| * возможность функционирования комплекса со следующими параметрами (на хост):
* до 12 TБ vMemory. Поддерживаются серверы архитектуры Intel x86-64 с конфигурацией до 160 логических процессоров, имеющих до 2 ТБ ОЗУ каждый. Эксплуатационно протестирована возможность функционирования комплекса с двукратным превышением параметров логических процессоров и количества задействованных процессоров в ВМ;
 |
| * возможность управления виртуальными ресурсами со следующими параметрами (на хост):
* до 1000 ВМ;
 |
| * поддержка встроенных механизмов, дающих возможность выделить виртуальным машинам больше оперативной памяти, чем физически есть на хосте;
 |
| * поддержка работы с оперативной памятью Memory Ballooning
 |
| 3 | Создание и управление виртуальными средами со следующей конфигурацией сети передачи данных: | Пользовательский портал для подключения пользователей к их виртуальным машинам. |
| Получение сеанса работы с ВМ по протоколам:* SPICE; VNC, RDP;
 |
| Клиент для предоставления рабочей среды «тонким клиентам» и ПК. |
| Параметры конфигурации сети передачи данных:маркировка QoS: 802.1p, DSCP; |
| поддержка возможности агрегации (логического объединения сетевых интерфейсов в соответствии со стандартом IEEE 802.3ad в режимах протоколов туннелирования уровней 2, 2+3, 3+4) сетевых соединений при построении сетевой инфраструктуры; |
| возможность подключения виртуальных машин к локальной сети на скорости 1/10 Гбит/с; |
| поддержка настраиваемых политик Teaming и Failover; |
| поддержка механизма Network I/O Control — приоритизации пулов ресурсов для сетевого трафика и поддержки стандарта 802.1q; |
| 4 | Создание и управление виртуальными средами со следующей конфигурацией систем хранения данных: | Поддержка инфраструктуры совместного хранения данных iSCSI, Gluster и NFS. |
| Возможность интеграции с внешними СХД без дополнительных лицензионных требований в базовой конфигурации |
| Параметры конфигурации систем хранения данных:поддержка блочного доступа к данным виртуальных машин по сети SAN по протоколу FC 8, 16 Гб/сек, FCIP: |
| поддержка блочного доступа к данным виртуальных машин по сети SAN по протоколу iSCSI (SW и HW); |
| поддержка файлового доступа к данным виртуальных машин по протоколу NFS; |
| поддержка HBA/SCSI-дисков гостевых ОС; |
| слияние/удаление мгновенных снимков без перезагрузки виртуальной машины; |
| автоматическая балансировка нагрузки между хранилищами; |
| поддержка технологии подключения узлов сети хранения данных с использованием нескольких маршрутов. |
| Atomic Test and Set (ATS) — возможность защиты метаданных тома как кластерной файловой системы в ситуациях, когда большое количество хостов имеют разделяемый доступ к одному хранилищу. |
| поддержка встроенных средств для доступа к хранилищу по нескольким путям; |
| поддержка технологии Thin provisioning, позволяющей выделять виртуальной машине место на системе хранения по мере необходимости; |
| поддержка технологии виртуальных томов, обеспечивающей возможность абстрагирования ресурсов для внешних систем хранения |
| 5 | Динамическое назначение ресурсов VM | Динамическое добавление и изъятие «на лету» вычислительных ресурсов vCPU (зависит от типа гостевой ОС) |
| Динамическое добавление и изъятие «на лету» вычислительных ресурсов vMemory (зависит от типа гостевой ОС) |
| Динамическое добавление и изъятие «на лету» виртуальных сетевых адаптеров vNIC (зависит от типа гостевой ОС) |
| 6 | Управление ресурсами платформы виртуализации | Реализация системы управления в виде виртуального ПАК или в виде отдельного приложения |
| Централизованное управление всей виртуальной инфраструктурой с помощью единой консоли управления |
| Централизованное управление несколькими площадками (в каждой из которых используется отдельный сервер управления для обеспечения независимости работы при сетевых сбоях между ЦОД) |
| Централизованное управление библиотекой шаблонов, образов дисков и ВМ |
| 7 | Контроль целостности виртуальных машин | Наличие контроллера целостности виртуальной инфраструктуры и ее конфигураций, способного останавливать запуск ВМ, если её целостность нарушена |
| 8 | Профилирование хостов | Сохранение известных, проверенных конфигураций хостов с целью их дальнейшего использования для упрощенного развертывания большого количества серверов |
| 9 | Авторизация пользователей средствами службы каталога LDAP | Использование учетных записей службы каталога LDAP для авторизации пользователей системы виртуализации |
| 10 | Возможность разбиения виртуальной ИС на сегменты для отдельного пользователя и (или) группы пользователей | Разбиение на сегменты позволяет группировать объекты виртуальной инфраструктуры (ВИ) по общему признаку и повышает надежность реализации матрицы доступа субъектов ВИ к объектам ВИ (матрицы доступа) |
| 11 | Возможность использования встроенного в гипервизор межсетевого экрана | Позволяет уменьшить поверхность атаки на гипервизор на сетевом уровне путем фильтрации сетевых подключений самим гипервизором |
| 12 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | Комплекс встроенных механизмов идентификации и аутентификации субъектов доступа и объектов доступа (ИАФ) повышают защищенность компонентов виртуализации при доступе администраторов и пользователей к объектам ВИ через центр управления виртуальной инфраструктурой и обеспечивает выполнение мер защиты информации:- Идентификация и аутентификация пользователей, являющихся работниками оператора;- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;- Защита обратной связи при вводе аутентификационной информации;- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей); |
| 13 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | Управление доступом субъектов доступа к объектам доступа (УПД), в том числе:* Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
* Реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
* Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
* Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
* Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
* Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
 |
| 14 | Регистрация событий безопасности в виртуальной инфраструктуре | * Регистрация событий безопасности (РСБ), в том числе:
* Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
* Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
* Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
* Защита информации о событиях безопасности;
* Контроль (анализ) защищённости информации (АНЗ)
* Наличие средства оповещения администратора безопасности СВ о событиях безопасности.
* Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться номер (уникальный идентификатор) события, дата, время, тип события безопасности.
* Записи журнала событий безопасности должны представляться структурированном виде и содержать время события безопасности, взятое аппаратной платформы или хостовой операционной системы.
* Регистрации подлежат как минимум следующие события безопасности:

успешные и неуспешные попытки аутентификации пользователей средства виртуализации;доступ пользователей средства виртуализации к виртуальным машинам;создание и удаление виртуальных машин;запуск и остановка средства виртуализации с указанием причины остановки;запуск и остановка виртуальных машин с указанием причины остановки;изменение ролевой модели;изменение конфигурации средства виртуализации;изменение конфигураций виртуальных машин;факты нарушения целостности объектов контроля. |
| 15 | Поддержка ролевой модели управления доступом (RBAC) | * Ролевая модель управления доступом позволяет назначать различным пользователям различные роли, обязанности, возможности управления, в том числе платформой виртуализации сетевых ресурсов и вводить для различных пользователей соответствующие ограничения. В пределах одной системы могут существовать до 64 ролей. Назначение пользователей на роли выполняется либо на локальном уровне, либо централизованно через активный каталог.
* Должен быть реализован ролевой метод управления доступом с четырьмя ролями пользователей:

разработчик ВМ, администратор безопасности СВ, администратор СВ администратор ВМ.* Роль администратора средства виртуализации должна позволять:

создавать учетные записи пользователей СВ;управлять учетными записями пользователей СВ;назначать права доступа пользователям средства виртуализации к ВМ;создавать и удалять виртуальное оборудование СВ;изменять конфигурации виртуального оборудования СВ;управлять доступом виртуальных машин к физическому и виртуальному оборудованию;управлять квотами доступа виртуальных машин к физическому и виртуальному оборудованию;управлять перемещением виртуальных машин;удалять виртуальные машины;запускать и останавливать виртуальные машины;создавать снимки состояния виртуальных машин, включающих файл конфигурации виртуальной машины, образа виртуальной машины и образа памяти виртуальной машины.* Возможность обеспечивать определения полномочий для пользователей средства виртуализации в пределах назначенных им ролей.
 |
| 16 | Централизованный аудит и формирование отчетов | Централизованный аудит и формирование отчетов должен обеспечивать:- возможность просмотра состояния и событий СУСВ, а также статистики получаемого к ВМ доступа пользователями;- возможность формирования и просмотра отчетов, связанных с работой кластера СУСВ и ее подсистем, ВМ и доступов к ним.А также должен обеспечивать формирование следующего минимума отчетов за отчетный период (день, неделя, месяц, год):- отчет об утилизации ресурсов на хостах (гипервизорах) за отчетный период;- отчет об утилизации ресурсов для ВМ за отчетный период;- о статистике простоя хостов (гипервизоров) в кластере за отчетный период;- об утилизации конкретного хоста (гипервизора) за отчетный период;- отчет о наличии и использовании свободного места по хранилищам СУСВ за отчетный период;- отчет о наличии и использовании ресурсов процессора в ЦОД, в кластере и хосте виртуализации за отчетный период;- отчет о наличии и использовании оперативного запоминающего устройства (далее – ОЗУ) в ЦОД, в кластере и хосте виртуализации за отчетный период; |

* + 1. Требования к функционалу виртуализации сетевых ресурсов

|  |  |  |
| --- | --- | --- |
| № | Функционал | Требования к функционалу |
| 1 | Перенос сетевого окружения, сетевых настроек и политик безопасности между ЦОД | Перенос виртуальных машин вместе с их сетевыми настройками и политиками безопасности между ЦОД, входящих в общую систему виртуализации |
| 2 | Поддержка распределенной коммутации уровня L2 | Предоставление возможности распределенной коммутации пакетов уровня L2 без привязки к нижележащей топологии сети и физическому расположению |
| 3 | Защита периметра (файрвол) | Возможность использования граничного файрвола с функцией фильтрации пакетов, защищающего сетевой периметр |
| 4 | Трансляция сетевых адресов (NAT) | Возможность транслирования сетевых адресов транзитных пакетов |
| 5 | Автоматизация предоставления персонализированной инфраструктуры, приложений и специализированных ИТ-услуг | Возможность предоставления:виртуальной машины с требуемым числом ядер ЦП, объёмом ОЗУ и параметрами надежности;дискового пространства на СХД с требуемыми параметрами производительности и надежности |
| Возможность построения отказоустойчивой и катастрофоустойчивой инфраструктуры IaaS («инфраструктура как услуга») за счёт использования встроенных средств обеспечения высокой доступности и автоматизированного аварийного переключения узлов платформы |
| Возможность обеспечения самообслуживания за счёт выбора ресурсов инфраструктуры и ИТ-услуг из единого каталога |
| Наличие функционала виртуализированных рабочих столов в базовой конфигурации |

* + 1. Требования к функционалу управления облачной виртуализованной инфраструктурой

|  |  |  |
| --- | --- | --- |
| № | Функционал | Требования к функционалу |
| 1 | Автоматизация предоставления персонализированной инфраструктуры, приложений и специализированных ИТ-услуг | Возможность предоставления виртуальной машины с требуемым числом ядер ЦП, объёмом ОЗУ и параметрами надежности |
| Возможность предоставления физического сервера с требуемым числом ядер ЦП и объёмом ОЗУ |
| Возможность предоставления дискового пространства на СХД с требуемыми параметрами производительности и надежности |
| Возможность построения отказоустойчивой и катастрофоустойчивой инфраструктуры IaaS за счёт использования встроенных средств обеспечения высокой доступности и автоматизированного аварийного переключения узлов платформы |
| Возможность обеспечения самообслуживания за счёт выбора ресурсов инфраструктуры и ИТ-услуг из единого каталога |

* + 1. Требования к взаимодействию со смежными системами

|  |  |  |
| --- | --- | --- |
| № | Функционал | Требования к функционалу |
| 1 | Интеграция с операционными системами | Возможность установки серверных операционных систем Microsoft Windows Server 2012 R2, Роса Кобальт, Роса Хром, RELD, RELS, Astra Linux, ALT Linux |
| 2 | Интеграция с аппаратными платформами | Поддержка серверных платформ x86 и x86-64 |
| 3 | Интеграция с системами мониторинга | Поддержка распространённых систем мониторинга. Поддержка стандартных протоколов безагентного мониторинга (SNMP, ICMP), поддержка мониторинга путем установки специализированных агентов |

* + 1. Требования к реализуемым мерам защиты

Система управления средой виртуализации должна реализовывать следующие требования к мерам защиты информации:

1) ИАФ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора;

2) ИАФ.2. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных;

3) ИАФ.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

4) ИАФ.4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

5) ИАФ.5. Защита обратной связи при вводе аутентификационной информации;

6) ИАФ.6. Идентификация и аутентификация пользователей, не являющихся работниками оператора;

7) УПД.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

8) УПД.2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

9) УПД.3. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

10) УПД.4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

11) УПД.6. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

12) УПД.10. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

13) УПД.11. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

14) УПД.12. Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки;

15) ОПС.4. Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов;

16) ЗНИ.1. Учет машинных носителей информации;

17) ЗНИ.2. Управление доступом к машинным носителям информации;

18) ЗНИ.3. Контроль перемещения машинных носителей информации за пределы контролируемой зоны;

19) ЗНИ.4. Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах;

20) ЗНИ.5. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации;

21) ЗНИ.6. Контроль ввода (вывода) информации на машинные носители информации;

22) ЗНИ.7. Контроль подключения машинных носителей информации;

23) ЗНИ.8. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);

24) РСБ.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения;

25) РСБ.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

26) РСБ.3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

27) РСБ.4. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

28) РСБ.5. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

29) РСБ.6. Генерирование временных меток и (или) синхронизация системного времени в информационной системе;

30) РСБ.7. Защита информации о событиях безопасности;

31) РСБ.8. Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе;

32) АНЗ.5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе;

33) ОЦЛ.1. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;

34) ОЦЛ.3. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

35) ОДТ.4. Периодическое резервное копирование информации на резервные машинные носители информации;

36) ОДТ.5. Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала;

37) ОДТ.6. Кластеризация информационной системы и (или) ее сегментов;

38) ЗСВ.1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации с учетом требований ГОСТ Р 58833-2020. "Защита информации. Идентификация и аутентификация. Общие положения";

39) ЗСВ.2. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

40) ЗСВ.3. Регистрация событий безопасности в виртуальной инфраструктуре;

41) ЗСВ.4. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;

42) ЗСВ.6. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

43) ЗСВ.7. Контроль целостности виртуальной инфраструктуры и ее конфигураций;

44) ЗСВ.8. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры, дополнительно должно обеспечиваться резервное копирование параметров настройки средства виртуализации, должно обеспечиваться резервное копирование сведений о событиях безопасности.

45) ЗСВ.10. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей;

46) ЗИС.1. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы;

47) ЗИС.10. Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам;

48) ЗИС.15. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации;

49) ЗИС.17. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы;

50) ЗИС.19. Изоляция процессов (выполнение программ) в выделенной области памяти;

51) ЗИС.21. Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы;

52) ЗИС.23. Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;

53) ЗИС.29. Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы.

* + 1. Требования к программной документации.
* Система управления средой виртуализации должна сопровождаться детальной программной документацией, исполненной на русском языке, и должна содержать следующие сведения:
* Руководство по установке системы виртуализации
* Руководство администратора по управлению и настройке системы виртуализации
* Руководство пользователя по эксплуатации системы виртуализации
* Формуляр на изделие
	+ 1. Требования к предоставлению гарантийной поддержки

Гарантийная поддержка оказывается сроком на 1 год.

|  |  |
| --- | --- |
| Количество Запросов в месяц | Без ограничений |
| Публикация обновлений ПО | Да |
| Предоставление личного кабинета на портале технической поддержки | Да |
| Каналы приема Запросов | Электронная почта,Портал технической поддержки |
| Время приема Запросов | КруглосуточноПо электронной почте и через портал технической поддержки |
| Время обработки Запросов | КруглосуточноПо электронной почте и через портал технической поддержки |
| Вопросы создания, оптимизации и использования инфраструктурных решений | Да |
| Вопросы по эксплуатации ПО, связанные с отсутствием соответствующей информации в документации, с некорректным (недокументированным) функционированием ПО или с необходимостью внесения исправлений в программный код ПО | Да |
| Прием сообщений об ошибках. | Да |
| Консультации по установке программного обеспечения сторонних производителей, не входящего в репозиторий | Да |

* 1. Требования к Внедрению системы виртуализации
		1. Общие требования

Модернизация виртуальной инфраструктуры должна включать в себя этапы развертывания, подключения технических средств под единое управление платформой виртуализации и миграцию виртуальных машин.

Исполнитель разрабатывает и согласовывает план график модернизации одного кластера, включающий этапы миграции серверов с ролью гипервизора, сервера централизованного управления и виртуальных машин.

Исполнитель разрабатывает и согласовывает имена и IP адреса, актуализирует схемы подключения технических средств.

Заказчик предоставляет:

* Актуальные сведения по настройкам используемой среды виртуализации;
* Актуальные схемы подключения технических средств;
* Актуальные сведения по назначенным и используемым ресурсам ВМ;
* Административные права доступа на технические средства текущей среды виртуализации;
* Административные права доступа на узлы текущей среды виртуализации;
* Сведения по IP адресации для настройки технических средств;
* Рабочее место для проведения работ с доступом в Интернет.

Заказчик обеспечивает:

* Предоставление необходимых технических средств для развертывания платформы виртуализации;
* Доступ в помещение и к техническим средствам сотрудникам Исполнителя.

Исполнитель обеспечивает:

* Миграцию всех серверов платформы виртуализации БАЗИС.DYNAMIX, в количестве 33 штук на среду виртуализации «Rosa –virtualization» сертифицированной ФСТЭК.
* неразглашение информации, ставшей ему известной в ходе выполнения работ;
* требований по конфиденциальности.
	+ 1. Требования к миграции серверов системы виртуализации на ПО виртуализации сертифицированную ФСТЭК

Миграция серверов системы виртуализации должна осуществляться согласно разработанного плана графика.

Система виртуализации должна функционировать только на технических средствах Заказчика.

Миграции подлежат сервера и сервер управления виртуальной инфраструктуры, функционирующие в текущей платформе виртуализации,

Исполнитель выполняет установку и настройку операционной системы и компонент системы виртуализации сертифицированной ФСТЭК:

* установку и настройку гипервизора на технические средства;
* настройку согласованной сетевой конфигурации;
* настройку кластера системы виртуализации;
* настройку дисковых ресурсов платформы виртуализации (дисковые ресурсы предоставляет Заказчик);
* настройку и проверку кластера виртуализации;

Исполнитель в ходе миграции обеспечивает:

* отказоустойчивое функционирование виртуальных машин, в случае выхода из строя одного из узлов кластера (сервер с ролью гипервизора) виртуальные машины успешно перезапускаются и функционируют на свободных ресурсах кластера;
* возможность миграции виртуальной машины между узлами кластера без необходимости остановки виртуальных машин;
* возможность переноса виртуальных жестких дисков между хранилищами без остановки виртуальных машин;
* централизованное управление объектами платформы виртуализации из единой консоли управления – управление узлами кластера, дисковыми доменами и сетевой инфраструктурой виртуализации;

управления виртуальной инфраструктурой с помощью защищенного протокола передачи данных HTTPS.

* + 1. Требования к обеспечению отказоустойчивой работы виртуальных машин в процессе модернизации виртуальной инфраструктуры

Миграция виртуальных машин должна осуществляться согласно разработанного плана графика.

Не допускается несогласованное выключение виртуальных машин.

Не допускается несогласованное мигрирование виртуальных машин.

Время недоступности и миграции виртуальных машин должно согласовываться и подтверждаться Заказчиком.

* 1. Требования Формирование документации по виртуальной инфраструктуре.
		1. Требования к документации средой виртуализации

Система управления средой виртуализации должна сопровождаться детальной программной документацией, исполненной на русском языке, и должна содержать следующие сведения:

1. Руководство по установке системы виртуализации
2. Руководство администратора по управлению и настройке системы виртуализации
3. Руководство пользователя по эксплуатации системы виртуализации
4. Формуляр на изделие
	* 1. Требования к инструкциям

Работы по модернизации виртуальной инфраструктуры должны быть проводиться по разработанным инструкциям.

В ходе выполнения модернизации инструкции должны актуализироваться с учетом инфраструктуры Заказчика.

* + 1. Требования к исполнительной документации

По результатам работ Исполнитель предоставляет Заказчику техническую документацию, содержащую:

* структурную схему работы виртуальной инфраструктуры;
* функциональную схему работы виртуальной инфраструктуры;
* пояснительную записку с описанием работы виртуальной инфраструктуры:
	+ имена, ip адреса серверов и системы хранения данных;
	+ список дисковых доменов и логических дисков СХД;

список ВМ.

Документация должна быть разработана с учетом требований стандарта ГОСТ 34.602-2020 "Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы".