Приложение 1

**Описание предмета закупки**

**«Передача неисключительных прав на использование программного обеспечения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры х86-64, уровень защищенности «Усиленный» («Воронеж»),**

**РУСБ.10015-01 (ФСТЭК)»\***

1. Передача неисключительных прав на использование программного обеспечения «Astra Linux Special Edition» (для рабочих станций)

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование показателя | Содержание (значение) показателя |
| 1 | Предмет закупки | Передача неисключительных прав на использование программ для ЭВМ ГАУЗ СО «Территориальный центр медицины катастроф». Лицензия на срок действия исключительного права с включенными обновлениями Тип 1 на 12 мес., программное обеспечение «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры х86-64, уровень защищенности «Усиленный» («Воронеж»), РУСБ.10015-01 (ФСТЭК) |
| 2 | Объем оказываемых услуг | Лицензия на 18 рабочих мест |
| 3 | Место поставки | 620036, Свердловская область, город Екатеринбург, Малопрудная ул., д. 6 |
| 4 | Срок (периодичность) передачи неисключительных лицензионных прав | Поставщик передает неисключительные лицензионные права Заказчику в срок не позднее 21 (двадцати одного) календарного дня в полном объеме с момента заключения договора |
| 5 | Условия поставки | Датой передачи неисключительных лицензионных прав, считается дата подписания Акта приема передачи неисключительных прав, без претензий |

# 1. Требования соответствия законодательным и нормативным документам

# 1.1. Программное обеспечение должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных согласно постановлению правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

# 1.2. Oперационная система должна иметь сертификат соответствия требованиям нормативных документов ФСТЭК России:

1.2.1. «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);

1.2.2. «Профиль защиты операционных систем типа «А» не ниже 4 класса ИТ.ОС.А4.ПЗ (ФСТЭК России, 2017);

1.2.3. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 4 уровня.

1.2.4. «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) не ниже 4 класса защиты.

1.3. Операционная система должна включать в свой состав сертифицированные средства контейнеризации, обеспечивающие изоляцию контейнеров, контроль целостности контейнеров и их образов, регистрацию событий безопасности, идентификацию и аутентификацию пользователей.

# 2. Требования к встроенному комплексу средств защиты информации операционной системы

2.1. Операционная система должна обеспечивать встроенными сертифицированными средствами:

2.1.1. управление средствами аутентификации;

2.1.2. управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям;

2.1.3. реализацию разграничения доступа;

2.1.4. возможность создания среды выполнения контейнеров и обеспечение работы с ними.

2.2. В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования.

2.3. В состав операционной системы должен входить комплекс программ объектно-реляционной защищённой СУБД с сертифицированными функциями безопасности.

2.4. В составе операционной системы должны быть графические средства ввода в домен.

2.5. Операционная система должна иметь графическое средство настройки ограничений пользователя по запуску программ в изолированном окружении с использованием механизма пространств имён и фильтрации системных вызовов, обеспечивающих:

2.5.1. ограничение прав пользователя на запуск приложений ядром системы;

2.5.2. ограничение прав пользователя средствами графического интерфейса;

2.5.3. разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности.

2.6. Обеспечение запрета запуска (исполнения) пользователем созданных самостоятельно (с использованием текстовых редакторов или непосредственно в командной строке) программ с использованием интерпретируемых языков программирования.

2.7. В составе операционной системы должны быть графические средства настройки защиты машинных носителей, обеспечивающие:

2.7.1. идентификацию устройств и сопоставление пользователя с устройством;

2.7.2. контроль подключения носителей информации;

2.7.3. учет носителей информации;

2.7.4. управление доступом к носителям информации;

2.7.5. контроль использования интерфейсов ввода/вывода информации;

2.7.6. ввод-вывод информации на носитель при условии совпадения маркировки носителя и объёма прав пользователя.

2.8. Операционная система должна включать в свой состав программное обеспечение, реализующее задачи аудита и журналирования (регистрации) событий безопасности.

2.9. Операционная система должна включать в состав графические средства контроля целостности:

2.9.1. контроль целостности дистрибутива;

2.9.2. контроль объектов файловой системы;

2.9.3. контроль целостности исполняемых файлов, обеспечивающий проверку их неизменности и подлинности.

2.10. В составе операционной системы должна быть реализована возможность ограничения полномочий пользователей по использованию консолей.

2.11. В составе операционной системы должно присутствовать ядро с функциями очистки и ограничения работы с оперативной памятью.

2.12. Должно быть обеспечено наличие регулярного включения информации об уязвимостях программного обеспечения операционной системы в банк данных угроз безопасности информации ФСТЭК России, устраняющих неисправности прикладного программного обеспечения и уязвимости операционной системы с подтверждением информации об исправленных уязвимостях путём размещения таких сведений в банке данных угроз безопасности информации ФСТЭК России (<http://bdu.fstec.ru/vul>).

2.13. Механизмами безопасности операционной системы должна быть обеспечена защита системных и привилегированных процессов от несанкционированного доступа и управления (исключение возможности повышения привилегий пользователей и управления привилегированными процессами в случае использования дефектов/уязвимостей в программном обеспечении информационной системы).

2.14. Операционная система должна обеспечивать запрет операций записи в системные каталоги и файлы (программы, файлы конфигурации), а также установки программного обеспечения, запуска и останова системных процессов операционной системы, вне зависимости от изменения пользователем своих привилегий в текущем сеансе работы.

2.15. Операционная система должна обеспечивать возможность контроля целостности исполняемых файлов и файлов библиотек: EXE, DLL, .NET 7

# 3. Требования к функциональным возможностям операционной системы

3.1. Операционная система должна быть предназначена для функционирования на средствах вычислительной техники с аппаратной платформой х86-64 включая процессоры Intel не ниже 10-го поколения.

3.2. Операционная система  должна иметь отдельный дистрибутив для процессорных архитектур: Байкал-М, Эльбрус (8С, 8СВ).

3.3. Операционная система должна поддерживать работу на ядре Linux версии не ниже 6.1.

3.4. Операционная система должна обеспечивать функционал в графическом исполнении:

3.4.1. наличие средств создания, настройки и управления несколькими служебными репозиториями используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы и автоматической публикацией в сети по протоколам http и ftp;

3.4.2. наличие графической утилиты управления драйверами nvidia, intel, radeon с возможностью выбора драйверов и возможностью восстановления драйверов при неудачной загрузке ОС;

3.4.3. наличие средств настройки выделяемых ресурсов памяти пользователям (квоты);

3.4.4. наличие графического инструмента для редактирования значения переменных окружения (изменять значение и описание переменных, удалять и объявлять переменные);

3.4.5. наличие графических средств настройки и изменения ориентации экрана в ручном или автоматическом режиме, с возможностью калибровки поворота, а также задания ориентации по умолчанию;

3.4.6. наличие графического инструмента управления регистрацией событий, включающий в себя управление сервисом системных событий, настройку ротации событий и настройку параметров сбора системных событий. Графическое средство просмотра системных событий;

3.4.7. наличие средств настройки сохранения и восстановления сессии пользователя (восстановление при старте запущенных программ и их расположения после полного отключения электропитания АРМ);

3.4.8. наличие средств настройки потребления электроэнергии (яркость экрана, потухание, выключение монитора, переход в ждущий режим, сон и гибернацию) в случае изменения настроек электропитания (питание от сети, питание от батареи, низкий заряд батареи);

3.4.9. наличие средств монтирования usb устройств по сети (usbip или аналог) для подключения к нескольким ПК;

3.4.10. наличие средств настройки одновременной работы нескольких сотрудников на одном ПК с разделяемыми профилями;

3.4.11. наличие средств создания системных отчётов, предназначенных для сбора, сжатия, сохранения и отправки в службу сопровождения диагностических данных о работе системы;

3.4.12. наличие средств запуска работы с удалёнными, отдельными и вложенными графическими сессиями;

3.4.13. наличие средств настройки планирования времени завершения работы без участия пользователя (завершение сессии, выключение АРМ, перехода в энергосберегающие режимы) с настройкой уведомления о событии;

3.4.14. наличие средств запуска приложений с изменением приоритета выполнения с возможностью запуска от имени другого пользователя;

3.4.15. наличие средств настройки параметров загрузчика операционной системы (загружаемая операционная система по умолчанию, передаваемые параметры ядра, таймаут для ожидания действий пользователя, выбора источника ввода данных при загрузке, выбор терминала для вывода информации);

3.4.16. наличие средств расчёта контрольных сумм файлов и их сравнения;

3.4.17. наличие инструментов поиска файлов по шаблону, по содержимому, по времени создания или изменения, а также размеру файла;

3.4.18. наличие средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, [tar.bz](http://tar.bz), tar.xz, iso);

3.4.19. наличие средств для оповещения пользователя о конфликте IP-адресов при подключении к сети;

3.4.20. наличие графических средств настройки системы, в том числе: установки и синхронизация времени; управления пользователями; просмотра системных журналов; настройки и обслуживания принтеров.

3.5. Операционная система должна поддерживать следующий функционал:

3.5.1. графический интерфейс, адаптированный под использование на портативных устройствах;

3.5.2. возможность подключения к сети wi-fi до входа в систему, а так же аутентификация в сети Wi-Fi с использованием смарт-карты;

3.5.3. наличие в репозитории операционной системы браузера из единого реестра российских программ для электронных вычислительных машин и баз данных;

3.5.4. поддержка управления настройками системы, приложениями и сервисами (включая контекстные меню) с помощью touchscreen (сенсорный экран) с возможностью автоматического отключения при подключении мышки;

3.5.5. возможность ввода аутентификационых данных пользователя при входе в систему и при разблокировке экрана с использованием виртуальной клавиатуры без необходимости дополнительных настроек;

3.5.6. наличие средств управления энергопотреблением портативного устройства в зависимости от состояния батареи/источника питания.

3.6. Операционная система должна обеспечивать поддержку файловых систем и сетевых протоколов:

3.6.1. ext2/3/4, fat, ntfs, iso9660, XFS, ZFS, BTRFS;

3.6.2. TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB;

3.6.3. поддержка стандарта ISO9660;

3.6.4. наличие средств подключения ресурсов WebDAV в качестве локальной файловой системы для возможности использования их стандартными приложениями операционной системы.

3.7. Операционная система должна обеспечивать возможность создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя.

3.8. Операционная система должна обеспечивать среду функционирования для сертифицированных средств криптографической защиты информации, предназначенных для создания и проверки электронной подписи, сквозного шифрования сетевых соединений и каналов связи, установления защищенного соединения и обмена зашифрованными данными.

3.9. Дополнительные функциональные компоненты:

3.9.1. клиентское ПО, для осуществления подключения по протоколу RDP;

3.9.2. агенты служб централизованного управления системой;

3.9.3. приложение для сканирования документов с возможностью пропуска пустых страниц;

3.9.4. средство для работы с архивами;

3.9.5. средство просмотра и редактирования файлов .pdf;

3.9.6. средство для эмуляции запуска исполняемых файлов .exe;

3.9.7. средства просмотра и редактирования графики и изображений;

3.9.8. средство оптического распознавания символов.

1. Передача неисключительных прав на использование программного обеспечения «Astra Linux Special Edition» (для сервера)

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование показателя | Содержание (значение) показателя |
| 1 | Предмет закупки | Передача неисключительных прав на использование программ для ЭВМ ГАУЗ СО «Территориальный центр медицины катастроф». Лицензия на срок действия исключительного права с включенными обновлениями Тип 1 на 12 мес., программное обеспечение «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры х86-64, уровень защищенности «Усиленный» («Воронеж»), РУСБ.10015-01 (ФСТЭК) |
| 2 | Объем оказываемых услуг | Лицензия на 1 сервер |
| 3 | Место поставки | 620036, Свердловская область, город Екатеринбург, Малопрудная ул., д. 6 |
| 4 | Срок (периодичность) передачи неисключительных лицензионных прав | Поставщик передает неисключительные лицензионные права Заказчику в срок не позднее 21 (двадцати одного) календарного дня в полном объеме с момента заключения договора |
| 5 | Условия поставки | Датой передачи неисключительных лицензионных прав, считается дата подписания Акта приема передачи неисключительных прав, без претензий |

1. Требования соответствия законодательным и нормативным документам

1.1. Программное обеспечение должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных согласно постановлению правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

1.2. OC должна иметь сертификат соответствия требованиям нормативных документов ФСТЭК России:

1.2.1 «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);

1.2.2 «Профиль защиты операционных систем типа «А» не ниже 4 класса ИТ.ОС.А4.ПЗ (ФСТЭК России, 2017);

1.2.3 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 4 уровня;

1.2.4 «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022) не ниже 4 класса защиты;

1.2.5 «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) не ниже 4 класса защиты.

1.3. Операционная система должна включать в свой состав сертифицированные средства виртуализации, обеспечивающие доверенную загрузку виртуальных машин, контроль целостности, регистрацию событий, управление доступом и другие функции безопасности, резервное копирование виртуальных машин и идентификацию пользователей.

1.4. Операционная система должна включать в свой состав сертифицированные средства контейнеризации, обеспечивающие изоляцию контейнеров, контроль целостности контейнеров и их образов, регистрацию событий безопасности, идентификацию и аутентификацию пользователей.

2. Требования к встроенному комплексу средств защиты информации операционной системы

2.1. Операционная система должна обеспечивать встроенными сертифицированными средствами:

2.1.1. управление средствами аутентификации;

2.1.2. управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям;

2.1.3. реализацию разграничения доступа;

2.1.4. возможность создания защищенной среды виртуализации;

2.1.5. возможность создания среды выполнения контейнеров и обеспечение работы с ними;

2.1.6. технологию контейнеризации с поддержкой изоляции процессов.

2.2. В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования.

2.3. В состав операционной системы должен входить комплекс программ объектно-реляционной защищённой СУБД с сертифицированными функциями безопасности.

2.4. В составе операционной системы должны быть графические средства создания единого пространства пользователей с целью реализации централизованного хранения информации об окружении пользователей и сетевой аутентификации через ldap и kerberos.

2.5. Операционная система должна иметь графическое средство настройки ограничений пользователя по запуску программ в изолированном окружении с использованием механизма пространств имён и фильтрации системных вызовов, обеспечивающих:

2.5.1. ограничение прав пользователя на запуск приложений ядром системы;

2.5.2. ограничение прав пользователя средствами графического интерфейса;

2.5.3 разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности.

2.6. Обеспечение запрета запуска (исполнения) пользователем созданных самостоятельно (с использованием текстовых редакторов или непосредственно в командной строке) программ с использованием интерпретируемых языков программирования.

2.7. В составе операционной системы должны быть графические средства настройки защиты машинных носителей, обеспечивающие:

2.7.1. идентификацию устройств и сопоставление пользователя с устройством;

2.7.2. контроль подключения носителей информации;

2.7.3. учет носителей информации;

2.7.4. управление доступом к носителям информации;

2.7.5. контроль использования интерфейсов ввода/вывода информации;

2.7.6. ввод-вывод информации на носитель при условии совпадения маркировки носителя и объёма прав пользователя.

2.8. Операционная система должна включать в свой состав программное обеспечение, реализующее задачи аудита и журналирования (регистрации) событий безопасности.

2.9. Операционная система должна включать в состав графические средства контроля целостности:

2.9.1. контроль целостности дистрибутива;

2.9.2. контроль объектов файловой системы;

2.9.3. контроль целостности исполняемых файлов, обеспечивающий проверку их неизменности и подлинности.

2.10. В составе операционной системы должна быть реализована возможность ограничения полномочий пользователей по использованию консолей.

2.11. В составе операционной системы должно присутствовать ядро с функциями очистки и ограничения работы с оперативной памятью.

2.12. Должно быть обеспечено наличие регулярного включения информации об уязвимостях программного обеспечения операционной системы в банк данных угроз безопасности информации ФСТЭК России, устраняющих неисправности прикладного программного обеспечения и уязвимости операционной системы с подтверждением информации об исправленных уязвимостях путём размещения таких сведений в банке данных угроз безопасности информации ФСТЭК России (<http://bdu.fstec.ru/vul>).

2.13. Механизмами безопасности операционной системы должна быть обеспечена защита системных и привилегированных процессов от несанкционированного доступа и управления (исключение возможности повышения привилегий пользователей и управления привилегированными процессами в случае использования дефектов/уязвимостей в программном обеспечении информационной системы).

2.14. Операционная система должна обеспечивать запрет операций записи в системные каталоги и файлы (программы, файлы конфигурации), а также установки программного обеспечения, запуска и остановки системных процессов операционной системы, вне зависимости от изменения пользователем своих привилегий в текущем сеансе работы.

2.15. Операционная система должна обеспечивать возможность контроля целостности исполняемых файлов и файлов библиотек: EXE, DLL, .NET 7

3. Требования к функциональным возможностям операционной системы

3.1. Операционная система должна поддерживать работу на ядре Linux версии не ниже 6.1.

3.2. Операционная система должна обеспечивать функционал в графическом исполнении:

3.2.1. наличие средств создания, настройки и управления несколькими служебными репозиториями используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы и автоматической публикацией в сети по протоколам http и ftp;

3.2.2. наличие графического инструмента управления регистрацией событий, включающий в себя управление сервисом системных событий, настройку ротации событий и настройку параметров сбора системных событий, графическое средство просмотра системных событий;

3.2.3. наличие графического инструмента для редактирования значения переменных окружения (изменять значение и описание переменных, удалять и объявлять переменные);

3.2.4. наличие графической утилиты управления и мониторинга компонентов подсистемы безопасности;

3.2.5. наличие средств расчёта контрольных сумм файлов и их сравнения;

3.2.6. наличие средств для оповещения пользователя о конфликте IP-адресов при подключении к сети;

3.2.7. наличие средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso).

3.3. Операционная система должна обеспечивать поддержку файловых систем и сетевых протоколов:

3.3.1. ext2/3/4, fat, ntfs, XFS, ZFS, BTRFS;

3.3.2. TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB;

3.3.3. поддержка стандарта ISO9660;

3.3.4. наличие средств организации распределенной файловой системы;

3.3.5. наличие средств подключения ресурсов WebDAV в качестве локальной файловой системы для возможности использования их стандартными приложениями операционной системы.

3.4. Операционная система должна обеспечивать среду функционирования для сертифицированных средств криптографической защиты информации, предназначенных для создания и проверки электронной подписи, сквозного шифрования сетевых соединений и каналов связи, установления защищенного соединения и обмена зашифрованными данными.

3.5. Операционная система должна обеспечивать возможность создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя.

3.6. Дополнительные функциональные компоненты:

3.6.1. web-сервер;

3.6.2. почтовые сервисы и системы передачи почты: Exim, Dovecot, Postfix или эквивалент;

3.6.3. средства мониторинга;

3.6.4. средства удаленного и терминального доступа: VNC, RDP(xRDP), RemoteApp (freerdp) или эквивалент;

3.6.5. сервер печати;

3.6.6. службы резервного копирования: Bacula, Rsync или эквивалент;

3.6.7. набор программ для воспроизведения аудио и видео файлов;

3.6.8. редактор растровой графики;

3.6.9. запись оптических дисков;

3.6.10. программа сканирования;

3.6.11. защищённый графический сервер X.Org Xserver или эквивалент;

3.6.12. рабочий стол;

3.6.13. системные библиотеки libc или эквивалент;

3.6.14. компилятор GCC или эквивалент;

3.6.15. QT или эквивалент.

\* В Описании предмета закупки отсутствуют слова «или эквивалент» в связи с необходимостью формирования и направления структурированного электронного медицинского документа «Карта вызова скорой медицинской помощи» в Реестр электронных медицинских документов, что может быть обеспечено только приобретаемым заказчиком ПО «Astra Linux Special Edition».