Согласовано:

Заместитель генерального директора

по общим вопросам АО «РСП ТПК КГРЭС»

_____ Е.А.Силимянкина

«15» февраля 2024г.

Утверждаю:

Главный инженер

АО «РСП ТПК КГРЭС»

_____ О.А. Петров

«12» февраля 2024г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Приобретение неисключительных прав на использование операционной системы специального назначения «Astra Linux Special Edition»

1. КРАТКОЕ ОПИСАНИЕ ЗАКУПАЕМЫХ ТОВАРОВ

1.1. Наименование и объем закупаемых товаров

Лицензия на право установки и использования операционной системы специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64 (очередное обновление 1.7), уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК) в количестве 23 шт.

1.2. Сроки поставки товаров

Начало поставки с момента заключения договора

Окончание поставки 31.12.2024 г.

Приобретение Лицензий будет осуществляться в течение 2024 года по заявкам Покупателя. Общее количество указано в Приложении № 1 к ТЗ.

.3. Возможность поставки аналогичных товаров.

Эквивалент не допустим на основании пп. а) п. 3 части 6.1 ст. 3 223-ФЗ в целях необходимости обеспечения совместимости ОС специального назначения «Astra Linux Special Edition с программным обеспечением, находящимся в эксплуатации у Заказчика

2. ОБЩИЕ ТРЕБОВАНИЯ

1. Требования соответствия законодательным и нормативным документам
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».
ОС должна иметь сертификат соответствия требованиям нормативных документов ФСТЭК России: • «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016); • «Профиль защиты операционных систем типа «А» не ниже 3 класса ИТ.ОС.А3.ПЗ (ФСТЭК России, 2017); • «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 3 уровня.
2. Требования к встроенному комплексу средств защиты информации операционной системы

Операционная система должна обеспечивать встроенными сертифицированными средствами:

- управление средствами аутентификации;
- управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям;
- реализацию дискреционного и мандатного разграничения доступа;
- возможность создания защищенной среды виртуализации;
- технологию контейнеризации с поддержкой изоляции процессов;
- возможность маркировки документов при выводе на печать;
- управление доступом к защищаемым ресурсам БД на основе иерархических и не иерархических меток доступа;
- функционирование браузера с учетом политик мандатного управления доступом;
- реализацию мандатного управления доступом к почтовым сообщениям, а также автоматическую маркировку создаваемых пользователем почтовых сообщений.

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

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

В составе операционной системы должна быть реализована возможность внедрения в сетевые пакеты протоколов IPv4 и IPv6 классификационных меток в соответствии с ГОСТ Р 58256-2018.В составе операционной системы должна быть реализована возможность внедрения в сетевые пакеты протоколов IPv4 и IPv6 классификационных меток в соответствии с ГОСТ Р 58256-2018 для обеспечения:

- организации сетевого взаимодействия прикладных процессов на основе их классификационных меток;
- фильтрации сетевого трафика на основе классификационных меток.

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.

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:

- ограничение прав пользователя на запуск приложений ядром системы;
- ограничение прав пользователя средствами графического интерфейса.

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

Обеспечение запрета запуска (исполнения) пользователем созданных самостоятельно (с использованием текстовых редакторов или непосредственно в командной строке) программ с использованием интерпретируемых языков программирования, кроме указанных явно администратором безопасности.

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

идентификацию устройств и сопоставление пользователя с устройством;
контроль подключения носителей информации;
учет носителей информации;
управление доступом к носителям информации;

контроль использования интерфейсов ввода/вывода информации; ввод-вывод информации на носитель при условии совпадения маркировки носителя и объёма прав пользователя.
Операционная система должна включать в свой состав программное обеспечение, реализующее задачи аудита и журналирования (регистрации) событий безопасности.
Операционная система должна включать в состав графические средства контроля целостности: • контроль целостности дистрибутива; • контроль объектов файловой системы; • контроль целостности исполняемых файлов, обеспечивающий проверку их неизменности и подлинности.
В составе операционной системы должна быть реализована возможность ограничения полномочий пользователей по использованию консолей.
Операционная система должна иметь наличие регулярного включения информации об уязвимостях программного обеспечения 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), согласно Регламенту включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России, который разработан в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и направлен на реализацию Положения о банке данных угроз безопасности информации, утвержденного приказом ФСТЭК России от 16 февраля 2015 г. № 9 (зарегистрирован Минюстом России 17 апреля 2015 г., рег. № 36901).
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).
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.
3. Требования к функциональным возможностям операционной системы
Операционная система должна быть предназначена для функционирования на средствах вычислительной техники с аппаратной платформой x86-64 (процессоры Intel не ниже 12-го поколения)
Операционная система должна поддерживать работу на ядре Linux версии не ниже 5.15
ОС должна обеспечивать функционал в графическом исполнении: • наличие средств создания и настройки служебных репозиториев используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы; • наличие средств настройки выделяемых ресурсов памяти пользователям (квоты);

- наличие графической утилиты для работы с электронной подписью с возможностью нанесения графического штампа на подписанный документ с указанием времени создания документа;
- наличие графической утилиты управления драйверами nvidia, intel, radeon с возможностью выбора драйверов и возможностью восстановления драйверов при неудачной загрузке ОС;
- 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;
- наличие графической утилиты управления и мониторинга компонентов подсистемы безопасности;
- наличие графической утилиты для редактирования маркера накладываемого на документы при маркировке печати;
- наличие средств настройки сохранения и восстановления сессии пользователя (восстановление при старте запущенных программ и их расположения после полного отключения электропитания АРМ);
- наличие средств настройки потребления электроэнергии (яркость экрана, потухание или выключение монитора, переход в ждущий режим, сон или гибернацию) в случае изменения настроек электропитания (питание от сети, питание от батареи, низкий заряд батареи);
- наличие средств монтирования usb устройств по сети (usbip или аналог);
- наличие средств настройки одновременной работы нескольких сотрудников на одном ПК с разделяемыми профилями;
- наличие средств создания системных отчётов, предназначенных для сбора, сжатия, сохранения и отправки в службу сопровождения диагностических данных о работе системы;
- наличие средств запуска работы с удалёнными, отдельными или вложенными графическими сессиями;
- наличие средств настройки планирования времени завершения работы без участия пользователя (завершение сессии, выключение АРМ, перехода в энергосберегающие режимы) с настройкой уведомления о событии;
- наличие средств запуска приложений с изменением приоритета выполнения, либо от имени другого пользователя;
- 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);
- наличие инструментов поиска файлов по шаблону, по содержимому, по времени создания или изменения, а также размеру файла;
- наличие средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso);
- наличие средств расчёта контрольных сумм файлов и их сравнения;
- наличие графических средств настройки системы, в том числе: установки и синхронизация времени; управления пользователями; просмотра системных журналов; настройки и обслуживания принтеров.

ОС предоставлять графический инструмент для настройки пользовательского окружения.

ОС должна поддерживать следующий функционал:
- наличие средств организации распределенной файловой системы;
- графический интерфейс, адаптированный под использование на портативных

устройствах;
- поддержка управления настройками системы, приложениями и сервисами (включая контекстные меню) с помощью touchscreen (сенсорный экран);
- наличие графических средств настройки и изменения ориентации экрана в ручном и/или автоматическом режиме, с возможностью калибровки поворота, а также задания ориентации по умолчанию;
- наличие виртуальной клавиатуры для возможности ввода аутентификационых данных пользователя при входе в систему и при разблокировке экрана;
- наличие средств управления энергопотреблением портативного устройства в зависимости от состояния батареи/источника питания;
- в составе операционной системы должно присутствовать ядро с функциями очистки и ограничения работы с оперативной памятью;
- наличие в составе операционной системы браузера из единого реестра российских программ для электронных вычислительных машин и баз данных.

ОС должна обеспечивать поддержку файловых систем и сетевых протоколов:
- ext2/3/4, fat, ntfs, iso9660, XFS, ZFS, BTRFS;
- TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB;
- наличие средств подключения ресурсов WebDAV в качестве локальной файловой системы для возможности использования их стандартными приложениями операционной системы;
- поддержка возможности создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя.

ОС должна иметь подтверждённую оценку совместимости в формуляре разработчика СКЗИ в соответствии с реализацией и эксплуатацией в среде ОС шифровальных (криптографических) средств защиты информации регулирующихся Федеральной службой безопасности Российской Федерации, в том числе Приказом ФСБ России от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», а так же поддерживать возможность установки и использования программного обеспечения **КриптоПро и VipNet Client**, включающего:

- средства криптографической защиты информации, предназначенные для создания и проверки электронной подписи в целях организации юридически значимого документооборота;
- средства криптографической защиты информации, предназначенные для сквозного шифрования сетевых соединений и каналов связи;
- средства установления защищенного соединения и обмена зашифрованными данными.

ОС должна иметь подтверждённую совместимость со средствами антивирусной защиты.

Дополнительные функциональные компоненты:
- клиентское ПО, для осуществления подключения по протоколу RDP;
- агенты служб централизованного управления системой;
- средство для работы с архивами;
- средство просмотра и редактирования файлов .pdf;
- средство для эмуляции запуска исполняемых файлов .exe;
- средства просмотра и редактирования графики и изображений;
- средство оптического распознавания символов.

Согласовано:

Начальник ПЭО		Н.А. Саламова	15.02.24
[должность]	[подпись]	[расшифровка]	[дата]
Специалист по проведению регламентированных закупок		Е.С. Решева	14.02.2024
[должность]	[подпись]	[расшифровка]	[дата]

Согласно ПЗ 2024

Ответственный исполнитель:

Инженер-электроник		И.М. Дубов	
[должность]	[подпись]	[расшифровка]	[дата]

информация для контактов:
тел: 89632179788,
e-mail: dubov_i@tpk-kgres.ru

Приложение № 1 к техническому заданию Приобретение неисключительных прав на использование операционной системы специального назначения «Astra Linux Special Edition»

Наименование	Количество шт.
Лицензия на право установки и использования операционной системы специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64 (очередное обновление 1.7), уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи электронный, для рабочей станции, без ограничения срока, с включенной технической поддержкой тип «ПРИВИЛЕГИРОВАННЫЙ» на 12 мес.	23