Техническое задание

**Наименование закупки:** **«Поставка программного комплекса и операционной системы».**

**Функционально-технические требования к Программному комплексу и операционной системе:**

Программный комплекс и операционная система должны быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Программный комплекс и встроенные в него программные модули и операционная система должны без разработки, закупки и установки в информационную систему Заказчика дополнительного программного обеспечения, реализовывать функции, представленные в таблице ниже:

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | Наименование | Описание требований | Количество |
| **1** | Лицензия на право установки и использования Программного комплекса не менее чем на 1 устройстве и операционной системы специального назначения для 64-х разрядной платформы на базе процессорной архитектуры x86-64 (ФСТЭК) не менее чем на 8 устройствах, способ передачи BOX, для сервера, без ограничения срока, с включенной технической поддержкой не менее 12 мес. | Аутентификация пользователей по протоколам LDAP(S) и Kerberos:поддержка возможности использования единого идентификатора для доступа ко всем разрешенным ресурсам и системам для решения задач строгой и сквозной аутентификации пользователей. | **2** |
| Управление конфигурацией домена* создание, редактирование и удаление сайтов[[1]](#footnote-1), управление параметром location идентификации сайта;
* ведение реестра серверов и ролей, привязка серверов домена к сайтам;
* отображение связанного графа топологии домена и состояния готовности домена;
* управление доступом путём делегирования прав на пользователей и группы пользователей;

управление репликацией между контроллерами доменами путём добавления нового контроллера домена и создания соответствующих соглашений о репликации между конкретными контроллерами домена. |
| Управление параметрами групповых политик:* возможность включения и отключения параметра, а также установка необходимых значений параметра групповой политики, которые будут применены на целевом компьютере или пользователе;
* создание, редактирование, удаление групповых политик;
* назначение групповых политик на подразделения;
* суммирование групповых политик согласно иерархии подразделений от вышестоящего к нижестоящему;
* возможность установки приоритета применения групповой политики в рамках назначенного подразделения;
* управление иерархией и составом параметров групповых политик;
* управление службами и группами служб HBAC;

управление командами SUDO и группами команд SUDO. |
| Управление Kerberos:* управление службами Kerberos, в том числе создание и удаление;

управление политиками билетов Kerberos. |
| Управление параметрами пользователей и групп:* управление параметрами новых пользователей и групп по умолчанию;

расширение списка атрибутов пользователя, в том числе создание атрибута карточки пользователя. |
| Управление доверительными отношениями с доменами Active Directory:* создание доверительных отношений с доменами Microsoft Active Directory;
* возможность аутентификации и авторизации под учетными записями пользователей Microsoft Active Directory в доменах под управлением Программного комплекса;

миграция объектов из Microsoft Active Directory с сохранением структуры вложенности объектов. |
| Управление организационной структурой, пользователями и компьютерами:* возможность настройки организационной структуры подразделений в иерархическом виде;
* управление организационными единицами;
* управление учетными записями пользователей и группами пользователей;

управление учетными записями компьютеров и группами компьютеров. |
| Удаленный доступ:удаленное подключение к рабочему столу пользователя. |
| Установка и обновление программного обеспечения:* управление группами ПО;
* управление репозиториями ПО, в том числе создание, редактирование, ведение версионности, удаление;
* создание заданий на установку и удаление ПО, в том числе на компьютеры выбранных подразделений и/или групп компьютеров;

управления параметрами программного обеспечения аналогично групповым политикам с возможностью применения на компьютерах выбранных подразделений. |
| Установка операционной системы (далее – ОС) по сети:* развертывание сервера установки;
* редактирование скриптов сценария установки;
* импорт конфигурации сценария установки;
* создание профилей компьютеров, на которые планируется осуществлять установку;
* выполнение установки на выбранных компьютерах;

ввод в домен и конфигурация рабочей станции после установки. |
| Управление службой разрешения имен:* управление прямыми и обратными DNS зонами;

управление перенаправлением dns запросов. |
| Управление службой динамической настройки узла (DHCP) |
| Управление службой синхронизации времени |
| Управление службой печати |
| Управление общим доступом к файлам:* создание, редактирование и удаление общих папок;

ограничение доступа к общим папкам. |
| Мониторинг:* управление службой мониторинга (журнал событий, визуализация мониторинга), в том числе развёртывание серверов мониторинга, ведений журнала событий;

оперативный мониторинг компонент Программного комплекса, в том числе контроль доступности и работоспособности компонентов, мониторинг ошибок репликации, постановка компонент на мониторинг. |
| Журналирование событий:управление параметрами сбора и хранения журналов событий. |
| Навигация и поиск объектов:* навигация иерархического типа;

поиск объектов (таких, как учетные записи пользователей, учетные записи персональных компьютеров, группы безопасности и рассылки, принтеры и др.). |
| Справочный центр:* наличие встроенного в Программный комплекс справочного центра на русском языке;

возможность доступа к справочному центру из любого компонента Программного комплекса. |
| **2** | Лицензия клиентская, на право подключения 1 устройства к Программному комплексу, способ передачи электронный, без ограничения срока, с включенной технической поддержкой не менее 12 мес. | Аутентификация пользователей по протоколам LDAP(S) и Kerberos:поддержка возможности использования единого идентификатора для доступа ко всем разрешенным ресурсам и системам для решения задач строгой и сквозной аутентификации пользователей. | **100** |
| Управление конфигурацией домена* создание, редактирование и удаление сайтов[[2]](#footnote-2), управление параметром location идентификации сайта;
* ведение реестра серверов и ролей, привязка серверов домена к сайтам;
* отображение связанного графа топологии домена и состояния готовности домена;
* управление доступом путём делегирования прав на пользователей и группы пользователей;

управление репликацией между контроллерами доменами путём добавления нового контроллера домена и создания соответствующих соглашений о репликации между конкретными контроллерами домена. |
| Управление параметрами групповых политик:* возможность включения и отключения параметра, а также установка необходимых значений параметра групповой политики, которые будут применены на целевом компьютере или пользователе;
* создание, редактирование, удаление групповых политик;
* назначение групповых политик на подразделения;
* суммирование групповых политик согласно иерархии подразделений от вышестоящего к нижестоящему;
* возможность установки приоритета применения групповой политики в рамках назначенного подразделения;
* управление иерархией и составом параметров групповых политик;
* управление службами и группами служб HBAC;

управление командами SUDO и группами команд SUDO. |
| Управление Kerberos:* управление службами Kerberos, в том числе создание и удаление;

управление политиками билетов Kerberos. |
| Управление параметрами пользователей и групп:* управление параметрами новых пользователей и групп по умолчанию;

расширение списка атрибутов пользователя, в том числе создание атрибута карточки пользователя. |
| Управление доверительными отношениями с доменами Active Directory:* создание доверительных отношений с доменами Microsoft Active Directory;
* возможность аутентификации и авторизации под учетными записями пользователей Microsoft Active Directory в доменах под управлением Программного комплекса;

миграция объектов из Microsoft Active Directory с сохранением структуры вложенности объектов. |
| Управление организационной структурой, пользователями и компьютерами:* возможность настройки организационной структуры подразделений в иерархическом виде;
* управление организационными единицами;
* управление учетными записями пользователей и группами пользователей;

управление учетными записями компьютеров и группами компьютеров. |
| Удаленный доступ:удаленное подключение к рабочему столу пользователя. |
| Установка и обновление программного обеспечения:* управление группами ПО;
* управление репозиториями ПО, в том числе создание, редактирование, ведение версионности, удаление;
* создание заданий на установку и удаление ПО, в том числе на компьютеры выбранных подразделений и/или групп компьютеров;

управления параметрами программного обеспечения аналогично групповым политикам с возможностью применения на компьютерах выбранных подразделений. |
| Установка операционной системы (далее – ОС) по сети:* развертывание сервера установки;
* редактирование скриптов сценария установки;
* импорт конфигурации сценария установки;
* создание профилей компьютеров, на которые планируется осуществлять установку;
* выполнение установки на выбранных компьютерах;

ввод в домен и конфигурация рабочей станции после установки. |
| Управление службой разрешения имен:* управление прямыми и обратными DNS зонами;

управление перенаправлением dns запросов. |
| Управление службой динамической настройки узла (DHCP) |
| Управление службой синхронизации времени |
| Управление службой печати |
| Управление общим доступом к файлам:* создание, редактирование и удаление общих папок;

ограничение доступа к общим папкам. |
| Мониторинг:* управление службой мониторинга (журнал событий, визуализация мониторинга), в том числе развёртывание серверов мониторинга, ведений журнала событий;

оперативный мониторинг компонент Программного комплекса, в том числе контроль доступности и работоспособности компонентов, мониторинг ошибок репликации, постановка компонент на мониторинг. |
| Журналирование событий:управление параметрами сбора и хранения журналов событий. |
| Навигация и поиск объектов:* навигация иерархического типа;

поиск объектов (таких, как учетные записи пользователей, учетные записи персональных компьютеров, группы безопасности и рассылки, принтеры и др.). |
| Справочный центр:* наличие встроенного в Программный комплекс справочного центра на русском языке;

возможность доступа к справочному центру из любого компонента Программного комплекса. |
| **3** | Лицензия на операционную систему для 64-х разрядной платформы на базе процессорной архитектуры х86-64, уровень защищенности Базовый (ФСТЭК), для рабочей станции, без ограничения срока, с включенной технической поддержкой не менее 36 мес. | 1. Требования соответствия законодательным и нормативным документамПрограммное 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».OC должна иметь подтверждение возможности её применения для построения информационных (автоматизированных) систем, обрабатывающих информацию ограниченного доступа в виде сертификатов соответствия требованиям нормативных документов:• «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);• «Профиль защиты операционных систем типа «А» (ФСТЭК России, 2017) не ниже 6 класса;• «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 6 уровня доверия.2. Требования к встроенному комплексу средств защиты информации операционной системыОперационная система должна обеспечивать встроенными средствами:• управление средствами аутентификации;• управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям;• реализацию разграничения доступа.В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования.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:• идентификация 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.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).3. Требования к функциональным возможностям операционной системыОС должна обеспечивать функционал в графическом исполнении:• наличие средств создания и настройки служебных репозиториев используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы и автоматической подписи пакетов имеющимся ключами;• наличие средств настройки выделяемых ресурсов памяти пользователям (квоты);• 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 средств расчёта контрольных сумм файлов и их сравнения по алгоритмам ГОСТ Р 34.11-2012, MD5, SHA1, SHA256;• 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 графических средств настройки системы, в том числе: установки и синхронизация времени; управления пользователями; просмотра системных журналов; настройки и обслуживания принтеров.ОС должна поддерживать следующий функционал:• 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.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 CSP 4.0, КриптоПро CSP 5.0, VipNet Client 4.0) 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.Основные компоненты в составе ОС:• ядро Linux с поддержкой процессоров Intel 11-го поколения;• средства создания и функционирования виртуальной инфраструктуры с графическим интерфейсом, обеспечивающим управление средой виртуализации;• механизм контейнеризации, обеспечивающий режим виртуализации и изоляции ресурсов на уровне ядра операционной системы (Docker или эквивалент);• комплекс программ объектно-реляционной защищённой СУБД. | **90** |
| **4** | Лицензия на операционную систему для 64-х разрядной платформы на базе процессорной архитектуры х86-64, способ передачи электронный, серверная до 2 сокетов, без ограничения срока, с включенной технической поддержкой не менее 12 мес. | 1. Требования соответствия законодательным и нормативным документамПрограммное 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».OC должна иметь подтверждение возможности её применения для построения информационных (автоматизированных) систем, обрабатывающих информацию ограниченного доступа в виде сертификатов соответствия требованиям нормативных документов:• «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);• «Профиль защиты операционных систем типа «А» (ФСТЭК России, 2017) не ниже 6 класса;• «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 6 уровня доверия.2. Требования к встроенному комплексу средств защиты информации операционной системыОперационная система должна обеспечивать встроенными средствами:• управление средствами аутентификации;• управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям;• реализацию разграничения доступа.В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования.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:• идентификация 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.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).3. Требования к функциональным возможностям операционной системыОС должна обеспечивать функционал в графическом исполнении:• наличие средств создания и настройки служебных репозиториев используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы и автоматической подписи пакетов имеющимся ключами;• наличие средств расчёта контрольных сумм файлов и их сравнения по алгоритмам ГОСТ Р 34.11-2012, MD5, SHA1, SHA256;• наличие средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso)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 CSP 4.0, КриптоПро CSP 5.0, VipNet Client 4.0) 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.Основные компоненты в составе ОС:• ядро Linux с поддержкой процессоров Intel 11-го поколения;• web-сервер Apache или эквивалент;• почтовые сервисы и системы передачи почты: Exim, Dovecot, Postfix или эквивалент;• средства мониторинга Zabbix или эквивалент;• средства удаленного и терминального доступа: LTSP, VNC, RDP, RemoteApp или эквивалент;• комплекс программ объектно-реляционной защищённой СУБД;• защищенный сервер печати;• службы резервного копирования: Bacula, Rsync или эквивалент;• система разграничения доступа к внешним устройствам;• аудит и журналирование событий безопасности;• набор программ для воспроизведения аудио и видео файлов;• редактор растровой графики;• запись оптических дисков;• программа сканирования;• защищённый графический сервер X.Org Xserver или эквивалент;• защищённый рабочий стол;• системные библиотеки libc или эквивалент;• компилятор GCC или эквивалент;• QT или эквивалент. | **1** |

**Состав поставки Программного комплекса:**

Программный комплекс должен состоять из серверной и клиентской лицензии.

Серверная лицензия должна предоставлять неисключительные права на использование Программного комплекса и включать в себя право установки Программного комплекса не менее чем на одном серверном устройстве, а также право установки операционной системы специального назначения, включенного в Единый реестр российских программ для электронных вычислительных машин и баз данных не менее чем на восьми устройствах (физических или виртуальных).

Клиентская лицензия должна предоставлять неисключительные права на использование Программного комплекса и включать в себя право не менее чем для одного соответствующего устройства на подключение к серверу Программного комплекса.

Комплект поставки серверной лицензии Программного комплекса должен включать в себя физический носитель с Программным комплексом и эксплуатационной документацией.

Комплект поставки клиентской лицензии Программного комплекса должен включать в себя доступ к электронному носителю с Программным комплексом.

1. Сайты — это объекты, представляющие одну или несколько подсетей TCP/IP с высокой надежностью и быстрыми сетевыми подключениями. [↑](#footnote-ref-1)
2. Сайты — это объекты, представляющие одну или несколько подсетей TCP/IP с высокой надежностью и быстрыми сетевыми подключениями. [↑](#footnote-ref-2)