Приложение А.

Задание на выполнение работ по внедрению ЕСК и КПО версий 1.4.1/1.7.3

**СОЗДАНИЕ И ВНЕДРЕНИЕ ТЕХНИЧЕСКИХ РЕШЕНИЙ ПО ИМПОРТОЗАМЕЩЕНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЕДИНОЙ СЛУЖБЫ КАТАЛОГОВ И ИМПОРТОЗАМЕЩЕНИЮ КОМПЛЕКСА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА АРМ ПОЛЬЗОВАТЕЛЕЙ АО РНПК**

Задание на выполнение работ

Данный документ описывает требования к выполнению работ по созданию и внедрению технических решений по импортозамещению программного обеспечения Единой службы каталогов комплекса и программного обеспечения на АРМ пользователей АО РНПК.

Обозначения и сокращения

| **Термин, сокращение** | **Определение** |
| --- | --- |
| ЕСК | Единая служба каталогов |
| MS AD | Microsoft Active Directory – программное обеспечение службы активного каталога производства компании Microsoft |
| КПО | Комплекс программного обеспечения – совокупность программных продуктов, состоящих из системного ПО, ПО защиты информации и прикладного ПО, совместимых между собой, функционирующих на АРМ пользователя. |
| DHCP | Протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP |
| DNS | Сетевая служба разрешения доменных имен в IP-адреса |
| LDAP(S) | Протокол для доступа к службе каталогов |
| NTP | Сетевой протокол для синхронизации внутренних часов сетевых устройств с использованием сетей с переменной латентностью |
| VLAN | Выделенный сегмент сети, включающий группу хостов, взаимодействующих в рамках единого широковещательного домена |
| Kerberos | Cетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними. |
| NTLM | Протокол проверки подлинности запроса и ответа, который использует три сообщения для аутентификации клиента в среде, ориентированной на соединение и четвертое дополнительное сообщение, если требуется проверка целостности. |
| АРМ | Автоматизированное рабочее место |
| СУБД | Система управления базами данных |
| ВМ | Виртуальная машина |
| Инфраструктурные сервисы | Комплекс базовых приложений и информационных систем, обеспечивающих работу ИТ-сервисов и Инфраструктуры |
| ИС, Информационная система | Совокупность вычислительных и сетевых ресурсов, реализующая заданные функции системы |
| ОС | Операционная система |
| Отечественная ОС | Операционной система, включенная в единый реестр российских программ для электронных вычислительных машин и баз данных и (или) единый реестр программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации |
| СПО | Свободное программное обеспечение |

# Общие сведения.

* 1. **Наименование выполняемых работ.**

Наименование выполняемых работ: «Создание и внедрение технических решений по импортозамещению Единой службы каталогов и программного обеспечения на АРМ пользователей АО РНПК»

* 1. **Наименование Заказчика и Исполнителя работ.**

Заказчиком работ является Акционерное Общество Российская Национальная Перестраховочная Компания (АО РНПК), адрес: 125047, г. Москва, ул. Гашека, дом 6 (далее по тексту Заказчик).

Функции представителя Заказчика выполняет Департамент информационных технологий АО РНПК.

Исполнитель работ выбирается в соответствии с закупочными процедурами АО РНПК.

* 1. **Основание для выполнения работ.**
	2. Основанием для выполнения работ является внутренний документ АО РНПК «Паспорт проекта «Импортозамещение»».
	3. **Место проведения работ.**

Работы проводятся на технологических площадках Заказчика, указанных в Таблице 1.

Работы могут проводиться в режиме удалённого подключения *либо на непосредственно на территории Заказчика*.

По согласованию с Заказчиком работы, требующие непосредственного взаимодействия с Инфраструктурой Заказчика, могут проводиться с использованием средств анализа, автоматизированного или автоматического сбора данных, администрирования и коллективной работы.

**Табл. 1. Адреса площадок Заказчика.**

| № п/п | Наименование площадки | Адрес  |
| --- | --- | --- |
| 1 | Основной ЦОД | г. Москва, 1-й Дорожный проезд, дом 3 строение 2 |
| 2 | Резервный ЦОД | г. Москва, Коровинское шоссе, дом 41 |
| 3 | Офис | г. Москва, ул. Гашека, дом 6 |

# Назначение и цели выполнения работ.

Создание технических решений по импортозамещению КПО и импортозамещению программного обеспечения ЕСК и ее технологической обвязки на программные продукты из реестра Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Целями выполнения работ по созданию технических решений по импортозамещению КПО и импортозамещению ПО ЕСК являются:

* снижение санкционных рисков для всей ИТ-инфраструктуры АО РНПК за счет импортозамещения ПО ЕСК и КПО;
* создание импортозамещённого «ядра» ИТ-инфраструктуры, перевод основных служебных информационных систем и сервисов на отечественные решения;
* Переориентация внутренних информационных систем и сервисов на работу с импортозамещённым ПО ЕСК;
* пересмотр основных архитектурных решений, принятых в ЕСК и требующих изменений в связи с изменением состава программных продуктов в составе ЕСК;
* Переориентация внутренних информационных систем и сервисов на работу с импортозамещённым КПО;
* перенос пользовательского рабочего окружения из операционных систем иностранного производства на отечественные КПО;

Целевыми работами по КПО данному заданию являются:

* Проведение исследования текущей ИТ-инфраструктуры перед началом работ;
* Поставка и внедрение полноценной замены Microsoft Active Directory и её технологической обвязки (DNS, DHCP, WSUS~~,~~ RADIUS, NTP, FS);
* Формирование КПО, используемого на АРМ Заказчика, на основе отечественного ПО;
* Проведение тестирования сформированного КПО на средствах заказчика;
* Оказание технической поддержки при эксплуатации КПО на 3 года.
* Предоставление обновлений для сформированного КПО в рамках оказания услуг технической поддержки;

# Технические требования.

* 1. **Общие требования.**

При создании ЕСК должны быть учтены следующие общие требования:

* в АО РНПК функционирует геораспределенная ЕСК на программном продукте Microsoft Active Directory;
* проведение работ не должно приводить к сбоям в инфраструктуре, текущей ЕСК и как следствие сбоям в автоматизированных и информационно-аналитических системах, использующих инфраструктурные сервисы ЕСК;
* импортозамещаяемая ЕСК должна быть построена с учетом всех площадок, указанных в таблице 1 пункта 1.4;
* работники ДИТ АО РНПК могут не иметь необходимой квалификации, но должны выступать в роли тестировщиков и приёмщиков создаваемых технических решений;
* аппаратные ресурсы (среда виртуализации) для проведения работ предоставляется АО РНПК.

При создании КПО должны быть учтены следующие общие требования:

* проведение работ не должно приводить к сбоям в ИТ-Инфраструктуре,
* КПО должен полностью заменять текущий набор ПО на АРМ пользователей АО РНПК;
* работники ДИТ АО РНПК могут не иметь необходимой квалификации, но должны выступать в роли тестировщиков и приёмщиков создаваемых технических решений;
* аппаратные ресурсы для проведения работ предоставляется АО РНПК.
	1. **Требования к функциям.**

В качестве целевого программного решения должен быть использован программный комплекс ALD Pro производства общества с ограниченной ответственностью «РусБИТех-Астра».

В качестве целевой серверной и десктопной операционной системы должна быть использована Astra Linux Special Edition не ниже версии 1.7 производства общества с ограниченной ответственностью «РусБИТех-Астра».

КПО должен взаимодействовать с программным комплексом ALD Pro производства общества с ограниченной ответственностью «РусБИТех-Астра».

Внедряемая ЕСК должна отвечать следующим инженерным требованиям.

* + - 1. **В части каталогов и единого входа должна обеспечивать:**
* предоставление единой точки аутентификации и авторизации пользователей на базе Kerberos;
* управление службами Kerberos, в том числе создание и удаление;
* управление политиками билетов Kerberos;
* предоставление единого, безопасного, надёжного и масштабируемого хранилища для всех объектов, размещённых в сети и поддерживающих интеграцию со службой каталогов (серверы, АРМ и т.д.);
* совместимость с NTLM/NTLMv2;
* репликация с другими серверами подсистемы;
* изменение структуры каталога при реорганизации;
* иметь возможность работы с системой с использованием командной строки;
* поддерживать локальную авторизацию при недоступности прочих контроллеров домена;
* иметь возможность создания служебных учетных записей для использования периферийным оборудованием, службами и системным ПО;
* встроенные механизмы обеспечения отказоустойчивости и высокой доступности;
* поддержку не более 2 (двух) территориально распределенных контроллеров службы каталога с возможным увеличением числа контроллеров в будущем;
* разделение географической и организационной структуры подразделений Заказчика в службе каталога;
* единую базу учетных записей;
* единый формат именования ресурсов;
* управление службами и группами служб HBAC;
* управление командами SUDO и группами команд SUDO;
* расчетное число пользователей службы каталога должно составлять не менее 1000 (семисот пятидесяти) пользователей с возможным увеличением количества обслуживаемых пользователей в будущем;
* непрерывное функционирование (24x7).
	+ - 1. **В части КПО должен отвечать следующим инженерным требованиям:**
* подключение к единой точке аутентификации и авторизации пользователей на базе Kerberos;
* взаимодействовать с политиками билетов Kerberos;
* поддержка протоколов SMB/SMB2/SMB3/CIFS (в том числе с поддержкой шифрования);
* совместимость с NTLM/NTLMv2;
* взаимодействовать со службами ALD Pro и другими серверными подсистемами;
* иметь возможность работы с системой с использованием командной строки;
* поддерживать локальную авторизацию при недоступности прочих контроллеров домена;
* иметь возможность создания служебных учетных записей для использования периферийным оборудованием, службами и системным ПО;
* встроенные механизмы обеспечения отказоустойчивости и высокой доступности;
* подключение к единой базе учетных записей;
* управление командами SUDO и группами команд SUDO;
* обеспечить централизованную установку/удаление, конфигурирование ПО;
* обеспечить централизованное обновления ПО и ОС АРМ;
* предоставление инструментальных средств для управления (с графическим интерфейсом и интерфейсом командной строки);
* поддержка шаблонных файлов;
* поддержка хранения информации в зашифрованном виде;
* поддерживать общий доступ к файлам SMB/CIFS, в том числе с парольной защитой;
* поддерживать совместное использование файлов;
* возможность настройки параметров общего доступа и уровней разрешения;
* поддерживать передачу данных по протоколам SMB/SMB2/SMB3/CIFS;
* возможность настройки правил доступа к каталогам с использованием учетных записей и групп службы каталога;
* поддерживать аутентификацию с использованием протокола Kerberos;
* поддерживать автоматизацию процесса развертывания на АРМ;
* поддерживать загрузку ОС по сети для бездисковой конфигурации компьютера;
* поддерживать разворачивание КПО по сети, без использования сменных носителей;
* КПО должна обеспечить механизм журналирования событий;
	+ - 1. **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 парольными политиками и политиками аудита.
	+ - 1. **Управление параметрами пользователей и групп:**
* централизованное создание, изменение и удаление аккаунтов пользователей, групп и других сущностей;
* возможность изменения существующих настроек группы;
* возможность добавления новых пользователей в группу с автоматическим применением настроек группы;
* управление параметрами пользователей и групп по умолчанию;
* расширение списка атрибутов пользователя, в том числе создание атрибута карточки пользователя.
	+ - 1. **Управление доверительными отношениями с доменами Active Directory:**
* создание исходящих доверительных отношений с доменами Microsoft Active Directory;
* возможность аутентификации и авторизации под учетными записями пользователей Microsoft Active Directory;
* миграция объектов из Microsoft Active Directory с сохранением структуры вложенности объектов подразделений.
* Запуск задач миграции объектов Microsoft Active Directory
* Подключение сетевых принтеров, подключенных к службе печати Microsoft Active Directory
* Должна быть реализована возможность миграции объектов из Microsoft Active Directory с сохранением структуры вложенности объектов. Для подразделений организации должна сохраняться иерархичность вложенности подразделений.
	+ - 1. **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;
* Управление подразделениями
	+ Создание подразделения
	+ Редактирование информации о подразделении
* Настройка иерархии подразделений в соответствии со структурой организации
	+ Добавление дочерних подразделений
	+ Привязка подразделений к вышестоящим подразделениям организации
* Управление пользователями и группами пользователей
	+ Создание групп пользователей
	+ Создание учетной записи пользователя
	+ Редактирование учетной записи пользователя
	+ Включение пользователя в группу пользователей
	+ Привязка пользователя к подразделению
* Управление компьютерами и группами компьютеров
	+ Создание групп компьютеров
	+ Редактирование учетной записи компьютера
	+ Включение компьютера в группу компьютеров
	+ Удаление учетной записи компьютера
	+ Удаление группы компьютеров
		1. **Обеспечение централизованного управления ИТ-инфраструктурой (в части управления АРМ) и обеспечивать следующий функционал:**
* централизованная установка/удаление, конфигурирование ПО;
* возможность централизованного обновления ПО и ОС АРМ;
* иметь возможность функционирования без использования агентов на целевых системах;
* возможность работать в режимах pull (запрос со стороны клиента) и\или push (уведомление со стороны сервера);
* возможность последовательного обновления состояния узлов (rolling update);
* предоставление инструментальных средств для управления (с графическим интерфейсом и интерфейсом командной строки);
* возможность создавать группы компьютеров разного назначения использования компьютеров с целью применения к ним различных групп автоматизированных задач;
* поддержка идемпотентного режима работы (многократное выполнение приводит к тому же результату, что и однократное выполнение);
* возможность расширения функционала путем добавления новых модулей;
* поддержка описания конфигураций систем в виде ролей;
* поддержка переменных и фильтров обработки переменных;
* поддержка шаблонных файлов;
* поддержка хранения информации в зашифрованном виде;
* иметь возможность составления графических отчетов по указанным задачам развертывания.
	+ 1. **ЕСК (в части DNS) должна обеспечивать:**
* предоставление информации об IP-адресах хостов по символьному адресу;
* поддержка настроек автоматического запуска обновлений DNS (nsupdate) клиентов при изменении их IP-адреса, поддержка актуальности записи DNS;
* поддержка настройки зоны DNS для синхронизации обратной записи клиента (PTR) вместе с прямой (A, AAAA) записью DNS;
* поддержка интеграции со службами LDAP и Kerberos;
* возможность переадресации между доменными именами;
* поддержку делегирования управления отдельными зонами и записями;
* возможность создания и управления зонами прямого и обратного просмотра;
* иметь поддержку записей типа A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV и TXT;
* иметь поддержку не менее 100 000 (Ста тысяч) записей типа A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV и TXT.
	+ 1. **Служба каталогов (в части DHCP-сервера) должна обеспечивать:**
* поддержка распространения сетевых параметров по протоколу DHCP;
* поддержка функции исключения IP-адресов из диапазона;
* поддержка функции привязки IP-адреса по MAC адресу;
* поддерживать отказоустойчивую конфигурацию;
* иметь возможность настройки опций, как на уровне всего сервера, так и на уровне пулов адресов;
* поддержка функции выдачи IP-адреса на определенный срок аренды.
	+ 1. **Служба общих файловых ресурсов должна:**
* поддерживать общий доступ к файлам SMB/CIFS, в том числе с парольной защитой;
* поддерживать совместное использование файлов;
* возможность настройки параметров общего доступа и уровней разрешения;
* поддерживать передачу данных по протоколам SMB/SMB2/SMB3/CIFS;
* возможность настройки правил доступа к каталогам с использованием учетных записей и групп службы каталога;
* поддерживать аутентификацию с использованием протокола Kerberos;
* поддерживать возможность дедупликации данных;
* иметь возможность квотирования каталогов на всех уровнях;
	+ 1. **ЕСК в части автоматизированного развёртывания образа операционной системы должна обеспечивать:**
* возможность централизованного хранения образов ОС;
* возможность централизованного управления образами ОС;
* возможность автоматизации процессов развертывания ОС на АРМ;
* возможность загрузки ОС по сети для бездисковой конфигурации компьютера;
* возможность загрузки образа ОС по сети, без использования сменных носителей;
* возможность выбора сервера хранения образов, во время развертывания ОС;
	+ 1. **ЕСК должна обеспечить управление службой синхронизации времени (NTP).**
* Управления синхронизацией времени контроллеров домена (NTP);
	+ Развертывание корневого NTP-сервера;
		1. **ЕСК должна обеспечить управление планировщиком заданий.**
		2. **ЕСК должна обеспечить аутентификацию и авторизацию по протоколу RADIUS.**
		3. **Поддерживать возможности внедрения внутреннего центра сертификации (CA).**
		4. **ЕСК должна обеспечить механизм журналирования событий.**
* Он должен позволять осуществлять журналирование событий ЕСК и их поиск и отображение с использованием визуального интерфейса ЕСК;
* управлять службой журналирования событий
	+ Развертывание серверов журналирования событий
	+ Настройка правил сбора событий
		1. **ЕСК должна обеспечить механизм навигации и поиска объектов.**
* Навигация по разделам ЕСК иерархического типа
* Поиск объектов внутри разделов ЕСК
	+ 1. **Операционные системы серверов ЕСК должны:**
* поддерживать работу с файловыми системами Ext 2/3/4, FAT, exFAT, NTFS, CIF, XFS, FAT32;
* поддерживать протоколы CIFS (SMB), NFS, FTP, SMB 2.0, SMB 3.0,;
* иметь утилиту для проверки и восстановления целостности файловых систем;
* иметь утилиту для создания и управления файловой системой;
* иметь утилиту, формирующую отчет о доступном и использованном дисковом пространстве на файловых системах;
* иметь утилиту, формирующую отчет об использовании дискового пространства заданными файлами, а также каждым каталогом иерархии подкаталогов каждого указанного каталога;
* включать в свой состав графические средства настройки операционной системы, включая аутентификацию, установку и синхронизацию времени, управление пользователями, группами, просмотром системных журналов и настройку периферийного оборудования;
* включать графическое средство настроек потребления электроэнергии такие как: яркость экрана, перевод в спящий (дежурный) режим или выключение монитора, переход системного блока в спящий (дежурный) режим, режим ожидания или выключения с сохранением состояния;
* поддерживать одновременную работу мониторов по следующим профилям:
	+ один монитор с графическим разрешением не менее 1920х1080 пикселей;
	+ один монитор с графическим разрешением не менее 3840х2160 пикселей;
	+ два монитора с графическим разрешением не менее 1920x1080 пикселей каждый;
	+ четыре монитора с графическим разрешением не менее 1920x1080 пикселей каждый;
	+ один монитор с графическим разрешением не менее 1920х1080 пикселей и второй монитор с графическим разрешением 3840х2160 пикселей;
* поддерживать работу с мультимедийными форматами и изображениями;
* иметь набор программ для воспроизведения аудио и видео файлов, в том числе потоковых видеотрансляций;
* обеспечивать графический терминальный доступ с использованием сертификатов открытого ключа электронной подписи клиента;
* обеспечивать графический терминальный доступ к терминальным фермам Microsoft Windows;
* обеспечивать работу в браузере;
* работа в браузере должна обеспечить подключение к современным ВКС системам, работающим через WebRTC;
* обеспечивать совместимость и исправное функционирование прикладного ПО Заказчика: Kaspersky Endpoint Security, CheckPoint Mobile Security, UserGate VPN Client, Staffcop, КриптоПро и другого прикладного ПО, выявленного на этапе исследований ИТ-Инфраструктуры Заказчика;
* включать средства, обеспечивающие механизмы централизованной авторизации по протоколам LDAP и LDAP+Kerberos;
* обеспечивать возможность подключения общих папок при авторизации пользователя домена Microsoft Active Directory Domain, без ввода логина/пароля;
* обеспечивать возможность для работы со средством централизованного управления конфигурациями серверов и рабочих станций в домене для обеспечения функции управления и контроля состояния в домене в режиме реального времени;
* обеспечивать совместимость с отечественными программно-аппаратными комплексами аутентификации и хранения ключевой информации, подтверждаемую взаимными сертификатами совместимости продуктов от производителей;
* обеспечивать среду исполнения для запуска Windows-приложений в выбранной операционной системе, включая возможность использования электронной подписи;
* иметь возможность запрета удаленного root-доступа (предоставление полного доступа с правами администратора) по паролю;
* обеспечить возможность хранения журнала событий ОС на АРМ и иметь возможность их удаленного просмотра.
	+ - 1. **Операционная система в составе КПО должны:**
* поддерживать работу с файловыми системами Ext 2/3/4, FAT, exFAT, NTFS, CIF, XFS, FAT32;
* поддерживать протоколы CIFS (SMB), NFS, FTP, SMB 2.0, SMB 3.0, TFTP;
* иметь утилиту для проверки и восстановления целостности файловых систем;
* иметь утилиту для создания и управления файловой системой;
* иметь утилиту, формирующую отчет о доступном и использованном дисковом пространстве на файловых системах;
* иметь утилиту, формирующую отчет об использовании дискового пространства заданными файлами, а также каждым каталогом иерархии подкаталогов каждого указанного каталога;
* включать в свой состав графические средства настройки операционной системы, включая аутентификацию, установку и синхронизацию времени, управление пользователями, группами, просмотром системных журналов и настройку периферийного оборудования;
* включать графическое средство настроек потребления электроэнергии такие как: яркость экрана, перевод в спящий (дежурный) режим или выключение монитора, переход системного блока в спящий (дежурный) режим, режим ожидания или выключения с сохранением состояния;
* поддерживать работу с не менее двумя мониторами графического разрешения не менее 1920x1080 пикселей, или один монитор с графическим разрешением не менее 1920х1080 пикселей и второй монитор с графическим разрешением 3840х2160 пикселей и с возможностью поворота экрана на 90 градусов,;
* поддерживать работу с мультимедийными форматами и изображениями;
* иметь набор программ для воспроизведения аудио и видео файлов, в том числе потоковых видеотрансляций;
* обеспечивать графический терминальный доступ с использованием сертификатов открытого ключа электронной подписи клиента;
* обеспечивать графический терминальный доступ к терминальным фермам Microsoft Windows;
* обеспечивать работу в браузере;
* работа в браузере должна обеспечить подключение к современным ВКС системам, работающим через WebRTC;
* обеспечивать совместимость и исправное функционирование прикладного ПО используемого на АРМ Заказчика: Kaspersky Endpoint Security, CheckPoint Mobile Security, Staffcop, веб-браузер Yandex.Browser, средства просмотра PDF, средства просмотра графических файлов, средства просмотра медиафайлов, офисный пакет LibreOffice , архиватор 7-ZIP и другого прикладного ПО, выявленного на этапе исследований ИТ-Инфраструктуры Заказчика;
* обеспечить совместимость с периферийным оборудованием Заказчика: usb-аудио гарнитуры Logitech, usb-видеокамеры Logitech, встроенные видеокамеры ноутбуков Lenovo X1 Carbon/ThinkBook 15ITLG2-G3, встроенные микрофоны и динамики ноутбуков Lenovo X1 Carbon/ThinkBook 15ITLG2-G3, встроенные веб-камеры Lenovo ThinkCentre All in One Gen4, встроенные стандартные usb-c док-станции Lenovo, Bluetooth и Wi-Fi модули ноутбуков и рабочих станций Lenovo, Wi-Fi модулей Tp-Link и другого оборудования, которое будет выявлено в результате обследования;
* обеспечивать совместимость работы с современными банк-клиентами с использованием Российской криптографии;
* включать средства, обеспечивающие механизмы централизованной авторизации по протоколам LDAP и LDAP+Kerberos;
* обеспечивать возможность подключения общих папок при авторизации пользователя домена Microsoft Active Directory Domain, без ввода логина/пароля;
* обеспечивать возможность для работы со средством централизованного управления конфигурациями серверов и рабочих станций в домене для обеспечения функции управления и контроля состояния в домене в режиме реального времени;
* обеспечивать совместимость с отечественными программно-аппаратными комплексами аутентификации и хранения ключевой информации, подтверждаемую взаимными сертификатами совместимости продуктов от производителей;
* обеспечивать среду исполнения для запуска Windows-приложений в выбранной операционной системе, включая возможность использования электронной подписи;
* иметь возможность запрета удаленного root-доступа (предоставление полного доступа с правами администратора) по паролю;
* обеспечить возможность хранения журнала событий ОС на АРМ и иметь возможность их удаленного просмотра.
	1. **Требования к защите информации.**
		1. Исполнитель должен организовать проведение опытной эксплуатации внедряемых решений.
		2. Исполнитель должен организовать проведение приемочных испытаний внедряемых решений.
		3. Внедряемое решение должно обеспечивать:
			1. **В части ЕСК:**
* резервирования программных средств серверов ЕСК, в том числе средств защиты информации на случай возникновения нештатных ситуаций;
* возможность восстановления серверов ЕСК в случае возникновения нештатных ситуаций;
* идентификацию и аутентификацию пользователей и инициируемых ими процессов;
* идентификацию и аутентификацию устройств;
* управление идентификаторами;
* управление средствами аутентификации;
* защиту аутентификационной информации при передаче;
* управление учетными записями пользователей;
* реализацию антивирусной защиты на серверах ЕСК;
* обновление базы данных признаков вредоносных компьютерных программ (вирусов) на серверах ЕСК;
* реализация модели управления доступом;
* разделение полномочий (ролей) пользователей;
* назначение минимально необходимых прав и привилегий;
* ограничение неуспешных попыток доступа к объектам ИТ-Инфраструктуры через ЕСК;
* блокирование сеанса доступа пользователя при неактивности;
* реализацию защищенного удаленного доступа;
* управление действиями пользователей до идентификации и аутентификации;
* регистрацию событий безопасности;
* защиту информации о событиях безопасности;
* контроль целостности программного обеспечения серверов ЕСК;
* контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;
* генерирование временных меток и (или) синхронизация системного времени;
* запрет несанкционированной удаленной активации периферийных устройств;
* получение обновлений программного обеспечения серверов ЕСК от доверенного источника;
* контроль целостности обновлений программного обеспечения серверов ЕСК;
* резервное копирование информационного обеспечения ЕСК.
	+ - 1. **В части КПО:**
* идентификацию и аутентификацию пользователей и инициируемых ими процессов;
* идентификацию и аутентификацию устройств;
* управление идентификаторами;
* управление средствами аутентификации;
* идентификацию и аутентификацию внешних пользователей;
* защиту аутентификационной информации при передаче;
* управление учетными записями пользователей;
* реализацию модели управления доступом;
* разделение полномочий (ролей) пользователей;
* назначение минимально необходимых прав и привилегий;
* ограничение неуспешных попыток доступа в информационную (автоматизированную) систему;
* блокирование сеанса доступа пользователя при неактивности;
* управление действиями пользователей до идентификации и аутентификации;
* реализация защищенного удаленного доступа;
* контроль доступа из внешних информационных (автоматизированных) систем;
* контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;
* контроль подключения съемных машинных носителей информации;
* генерирование временных меток и (или) синхронизация системного времени;
* регистрацию событий безопасности;
* защиту информации о событиях безопасности;
* реализацию антивирусной защиты;
* обновление базы данных признаков вредоносных компьютерных программ (вирусов);
* контроль целостности программного обеспечения;
* разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями;
* защиту информации при ее передаче по каналам связи;
* обеспечение доверенных канала, маршрута;
* управление сетевыми соединениями;
* установку (инсталляцию) только разрешенного к использованию программного обеспечения;
* поиск, получение обновлений программного обеспечения от доверенного источника;
* контроль целостности обновлений программного обеспечения;
* установку обновлений программного обеспечения.
	1. **Требования к эргономике и технической эстетике**
* Взаимодействие пользователей с программным обеспечением, входящим в состав КПО и ЕСК должно осуществляться посредством визуального графического интерфейса (WebUI и /или GUI). Перечень функций доступный через различные интерфейсы определяется на этапе внедрения Системы. Графический интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к необходимым функциям и операциям.
* Пользовательские интерфейсы КПО и ЕСК должны адаптироваться/разрабатываться с учетом специфики повседневной работы системных администраторов.
* Графический интерфейс должен быть рассчитан на использование манипулятора типа «мышь», то есть управление должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов с минимизацией количества операций, выполняемых системным администратором.
* Клавиатурный режим ввода должен использоваться главным образом при выполнении функций в интерфейсе командной строки. В графическом интерфейсе при заполнении и/или редактировании текстовых и числовых полей экранных форм.
* КПО и ЕСК должны обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями системных администраторов, неверным форматом или недопустимыми значениями входных данных.
* Графический интерфейс, там, где он используется, должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм.
* При отображении многострочных массивов информации, выходящих за рамки экрана, должна показываться полоса прокрутки.
* На формах где используются списки должна быть возможность сортировки и фильтрации данных.
* Экранные формы должны отражать всю информацию и элементы оформления при разрешении экрана не менее 1024х768 с использованием стандартного шрифта.
* Элементы управления КПО и ЕСК должны адаптироваться под контекст операции. Например, элементы выполнения групповых операций должны отображаться только при выборе нескольких элементов из списка.
* Для полей ввода и элементов управления должны применяться текстовые подсказки и пояснения.
* Все поясняющие надписи в экранных формах, а также сообщения, выдаваемые пользователю (кроме системных сообщений), должны быть выполнены на русском языке.
* Справочная информация по работе с прикладным и системным ПО должна находиться непосредственно в КПО или ЕСК и позволять обратиться к ней. Справочная информация должна быть представлена на русском языке.

# Требования к составу и содержанию работ.

* + 1. **Требования к обследованию и анализу Инфраструктуры.**

Границами работ по обследованию и анализу Инфраструктуры Заказчика являются ЕСК и АРМ, ее технологическая обвязка, протоколы и процессы их взаимодействия ЕСК с инфраструктурными сервисами, информационными системами, системой информационной безопасности АО РНПК, АРМ пользователей и в внешними сетями связи, обеспечивающие штатное функционирование Инфраструктуры и рабочие станции Заказчика.

Заказчик предъявляет к исследованию не более 30 ИС и не более 5 типовых конфигураций АРМов.

Параметры штатного функционирования Инфраструктуры Заказчика определяются Исполнителем на этапе 01 путем интервьюирования сотрудников Заказчика или с применением технических средств диагностики и анализа, включаются в отчет об обследовании и анализе ПО ЕСК, а также связанных с ним информационных систем, инфраструктурных сервисов, компонентов системы информационной безопасности и АРМ.

Для каждого вида программного обеспечения АРМ и инфраструктурных сервисов Исполнитель подготавливает проект описания штатного функционирования данного решения на основании публичной и технической информации о данном решений и уточняет у Заказчика фактические показатели параметров штатного функционирования программного обеспечения на площадках Заказчика.

Перечень мероприятий, которые должен выполнить Исполнитель при обследовании Инфраструктуры Заказчика:

* сбор информации об Инфраструктуре АРМ Заказчика, включая, но не ограничиваясь, составом и настройками операционной системы, прикладного программного обеспечения, системного программного обеспечения, программного обеспечения для функционирования банк-клиентов, СКЗИ, оборудование рабочих мест, периферийное оборудование;
* сбор информации о составе и настройках виртуальных машин серверов ИТ-Инфраструктуры и Информационных систем АО РНПК, включая, но не ограничиваясь, составом и настройками операционной системы, прикладного программного обеспечения, системного программного обеспечения, СКЗИ, СУБД;
* сбор информации о взаимодействии ЕСК с компонентами системы информационной безопасности;
* сбор данных об адресном плане ИТ-инфраструктуры Заказчика;
* сбор данных о схеме, протоколах и технологиях взаимодействия компонентов/модулей/подсистем ИТ-инфраструктуры Заказчика между собой и с внешними системами и сетями.

На основании данных отчёта Исполнитель разрабатывает техническое задание для внедрения ЕСК и КПО на базе импортозамещенного программного обеспечения согласно требованиям разделов 3 и 4 настоящего задания.

* + 1. **Требования к проектированию инфраструктуры ЕСК и КПО**

При проектировании инфраструктуры ЕСК и КПО необходимо учитывать:

* необходимость выбора оптимальных программных решений, обеспечивающих переход Заказчика на преимущественное использование российского программного обеспечения;
* подготовку технических и организационных решений для организации целевой продуктивной среды;
* подготовку технических и организационных решений по тиражированию проектных решений для обеспечения перехода Заказчика на преимущественное использование российского программного обеспечения;
* подготовку технических и организационных решений по обеспечению миграции Инфраструктуры Заказчика на преимущественное использование российского программного обеспечения.
	+ 1. **Требования к программному обеспечению**

Все программное обеспечение, включаемое в проектное решение и КПО, должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных, с возможностью обеспечения техническое поддержки данного программного обеспечения правообладателем или уполномоченного им лицом.

Допускается применение свободно распространяемого программного обеспечения в случае отсутствия альтернативных решений в едином реестре российских программ.

* + 1. **Требования к разработке проектного решения инфраструктуры ЕСК**

При проектировании следует разработать комплект документов, приведённых в Табл. 1.

**Табл.2 – Состав документации для внедрения решений по настоящему Заданию на выполнение работ.**

| № пп | Наименования разрабатываемых документов | Требования к документам |
| --- | --- | --- |
| 1 | Аналитический отчёт о проведённых исследованиях ИТ-инфраструктуры и рабочих мест Заказчика | Н/Д |
| 2 | Календарный план | Н/Д |
| 3 | Техническое задание на разработку и внедрение ЕСК на базе отечественного программного обеспечения. | ГОСТ 34.201-89 |
| 4 | Техническое задание на разработку и внедрение КПО на базе отечественного программного обеспечения.  | ГОСТ 34.201-89 |
| 4 | Пояснительная записка | РД 50-34.698-90 |
| 5 | Спецификация(ии) оборудования и программных продуктов | ГОСТ 34.201-89 |
| 6 | Схема структурная комплекса технических средств | ГОСТ 34.201-89РД 50-34.698-90 |
| 7 | Таблица(ы) настроек | РД 50-34.698-90 |
| 8 | Программа и методика испытаний  | ГОСТ 34.603-92 |
| 9 | Форма протокола проведения испытаний | Н/Д |

* + 1. **Требования к разработке ПМИ**

Программа и методика проведения приемо-сдаточных испытаний должна включать следующие проверки:

* Оценку и установление факта достижения требований к успешности выполнения работ;
* соответствие функционирования внедряемых решений параметрам штатного функционирования программного обеспечения на площадках Заказчика;
* соответствие внедряемых решений требованиям проектного решения;
* соответствие внедряемых решений требованиям Задания на выполнение работ;
* комплектность и качество документации.

Программа и методика приемо-сдаточных испытаний предоставляется Исполнителем на согласование и утверждение Заказчику не позднее, чем за 30 (тридцать) рабочих дней до планируемой даты начала проведения приемо-сдаточных испытаний. Согласование осуществляется посредством направления ответственными представителями сторон электронных писем.

* + 1. **Требования к разработке формы протокола испытаний в соответствии с ПМИ**

Форма протокола испытаний должна отражать шаблон, включающий наименование всех проверок, предусмотренных ПМИ, форму для заполнения фактически выполненных действия по проверке и форму для внесения результата.

* + 1. **Требования к составу работ по настройке инфраструктуры ЕСК**
* обеспечить параллельное внедрение решений, описанных в проектном решении;
* не допустить нарушения штатного функционирования текущей ИТ-инфраструктуры;
* установить и настроить на виртуальной инфраструктуре, предоставленной Заказчиком, операционные системы и программное обеспечение для организации работы с новых инфраструктурных сервисов в соответствии с проектным решением;
* предоставить требования к настройке межсетевых экранов для реализации штатной работы всего внедряемого функционала;
* обеспечить сквозную аутентификацию и авторизацию работников на создаваемой и существующей ЕСК Заказчика;
* обеспечить миграцию конечных устройств Заказчика на использование внедряемых решений;
	+ 1. **Требования к составу работ по разворачиванию КПО**
* обеспечить параллельное внедрение решений, описанных в проектном решении;
* не допустить нарушения штатного функционирования текущей ИТ-инфраструктуры;
* обеспечить миграцию конечных устройств Заказчика на использование внедряемых решений;
* развернуть сервер установки КПО по сети;
* создать и отредактировать скрипты сценария установки:
	+ - * preseed
			* postinstall
			* boot-меню
			* первого запуска
			* ввода в домен и конфигурации рабочей станции после установки;
* импортировать конфигурации сценариев установки ОС файлом;
* Обеспечить ведение версионности изменений скриптов сценариев установки КПО;
* адаптировать устанавливаемые ОС под СПО и ППО, используемое Заказчиком;
* адаптировать интерфейс ОС согласно требованиям Заказчика (иконки, звуки, темы оформления и стили, шрифт, размеры шрифта, удаление/отключение неиспользуемого в бизнес-деятельности ПО и функционала системы);
* Создание профилей компьютеров, на которые планируется осуществлять установку КПО (не более 10 штук);
* выполнение установки на выбранных компьютерах (массовой установкой занимаются работники Заказчика);
	+ 1. **Требования к разработке календарного плана проекта.**

Исполнитель должен разработать и утвердить календарный плана и проект технического задания на осуществление поэтапного перехода Заказчика на преимущественное использование российского программного обеспечения для инфраструктуры рабочих мест, а также связанных с ними информационных систем и инфраструктурных сервисов, в соответствии с согласованным проектным решением.

* + 1. **Требования к устранению выявленных недостатков.**

В рамках проведения работ Исполнитель должен проводить работы по устранению выявленных недостатков по решению задач эксплуатацию и технической поддержки внедряемых решений инфраструктуры ЕСК и рабочих мест, а так же связанных с ними информационных систем и инфраструктурных сервисов.

При необходимости Исполнитель подключает техническую поддержку производителей решений.

Устранение происходит в рабочие часы.

* + 1. **Требования к гарантийным обязательствам на внедряемые решения.**

Исполнитель устанавливает гарантийный срок на внедряемые решения, проведённые работы и поставляемые товары в рамках данного Задания на выполнение работ сроком 12 месяцев.

* + 1. **Спецификация программных продуктов, необходимых для выполнения работ по данному задания указана в Табл 2.**

**Табл 2. Спецификация программных продуктов.**

| № пп | Артикул | Производитель | Наименования разрабатываемых документов | Количество | Комментарий |
| --- | --- | --- | --- | --- | --- |
| 1 | AD1200Х8610DIG000SR01-ST12 | Русбиттех | Лицензия на право установки и использования Программного комплекса ALD Pro РДЦП.10101-01 на 1 устройстве и операционной системы специального назначения Astra Linux Special Edition для 64-х разрядной платформы на базе процессорной архитектуры x86-64 РУСБ.10015-01 (ФСТЭК) на 8 устройствах, способ передачи электронный, для сервера, без ограничения срока, с включенной технической поддержкой тип Стандарт на 12 мес. | 2 |  |
| 2 | OS1000Х8617DIGALDWS01-ST12 | Русбиттех | Лицензия на право установки и использования операционной системы специального назначения Astra Linux Special Edition для 64-х разрядной платформы на базе процессорной архитектуры х86-64, вариант лицензирования Орел, РУСБ.10015-10, способ передачи электронный, для рабочей станции и лицензия клиентская на право подключения 1 устройства к Программному комплексу ALD Pro РДЦП.10101-01, способ передачи электронный, без ограничения срока, с включенной технической поддержкой тип Стандарт на 12 мес. | 250 |  |
| 3 | OS1101Х8617DIG000VS01-ST12 | Русбиттех | Лицензия на право установки и использования операционной системы специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры х86-64 (очередное обновление 1.7), уровень защищенности «Усиленный» («Воронеж»), РУСБ.10015-01 (ФСТЭК), способ передачи электронный, для 1 виртуального сервера, без ограничения срока, с включенной технической поддержкой тип "Стандарт" на 12 мес. | 10 |  |

* 1. **Требования к нормативным документам.**

При выполнении работ должны быть учтены требования следующих нормативных актов:

* Постановление 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»;
* Постановление Правительства Российской Федерации от 23.03.2017 г. № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных»;
* ГОСТ 34.201-89, Информационная технология, Виды, комплектность и обозначение документов при создании автоматизированных систем;
* ГОСТ 34.603-92, Информационная технология, Виды испытания автоматизированных систем;
* РД 50-34.698-90, Информационная технология, Требования к содержанию документов;